



**Lab Test Report
DR100409D**

Cisco CleanAir Competitive Testing



April 2010

Miercom
www.miercom.com

Contents

- Executive Summary 3
- Key Findings 4
- Overview 5
 - Test Bed Diagram 6
 - How We Did It 6
- Impact of Interference 7
 - Figure 1: 5.0GHz Baseline Measurements with Impact of Interference on Throughput 7
 - Figure 2: 2.4GHz Baseline Measurement with Impact of Interference on Throughput 8
- Interference Classification 9
 - Screen shot from Cisco 10
 - Screen shot from Motorola 11
 - Multiple Sources of Interference – 2.4GHz Band 12
 - Single Interferers – 5GHz Band 12
 - Figure 3: Classification and Information on Interferers by Cisco CleanAir and Motorola AirDefense 13
- Rogue Devices on Non-Standard Channels 14
- Self-Healing 15
 - Figure 4: Summary of Self-Healing Tests between Cisco CleanAir and Other Competitors 18

Executive Summary

Our independent third-party evaluation found Cisco CleanAir technology to be a comprehensive and valuable solution for resolving interference problems caused by non-Wi-Fi sources of interference in wireless networks.

Common non-Wi-Fi devices operating in the same radio spectrum as wireless networks can cause significant degradation of user quality of experience, high latency, and in some cases, complete disruption of the wireless network. This is due to the design of 802.11 as a polite protocol that uses a listen-before-talk algorithm. This design can allow the channel to be completely jammed by interference, resulting in dropped clients. The ability to identify and avoid these types of interference is of great importance to network managers.

Cisco CleanAir technology utilizes a custom radio ASIC in the access point to provide class-leading spectrum analysis and interference mitigation tools not available in standard Wi-Fi chipsets. These tools enhance the granularity of scanning resolution, and provide rapid avoidance of poor channel conditions to protect the end user experience.

We were pleased with the speed and accuracy of detection of various common sources of non-Wi-Fi interference, and particularly with the level of actionable information provided to assist in mitigation activities. Cisco CleanAir provided unique identifiers for each interference source, displayed the level of severity and air quality, correctly classified the type of device, and mapped the physical location of the source. The ability to identify and locate multiple simultaneous sources of interference was impressive.

CleanAir also demonstrated a unique advantage over competitors with self-healing by reliably changing to a clean channel in less than a minute to avoid interference from sources as far as 100 feet away. Another benefit was its ability to detect rogue access points hiding on a non-standard frequency that could pose a security threat to the network.

Vendors of competitive products did not actively participate in the testing included in this report. However all vendors are afforded an opportunity to demonstrate their product in testing to our labs if they disagree with any of the findings we presented.

Miercom is proud to present the Performance Verified Certification for the performance and integration of interference mitigation features as demonstrated by Cisco CleanAir technology.

Rob Smithers
CEO
Miercom

Key Findings

- Non-Wi-Fi interference can affect throughput between access points and clients in the 2.4GHz and 5GHz spectrum
- Cisco CleanAir technology detects, classifies, and maps locations of interference providing for rapid remediation
- A custom CleanAir ASIC in the Cisco Aironet 3500 Series Access Point (AP) provides scanning and detection advantages not available in other Wi-Fi chipsets
- CleanAir provides advanced detection of off-frequency rogue devices preventing backdoor security threats
- Rapid self-healing capability with interference avoidance provides improved end-user experience and quick recovery from channel interference
- Competitive analysis of the Motorola AirDefense product revealed it to be accurate in less than 25% of the test cases. (Mistaken identification 15%; intermittent detection 23%; missed or incomplete classification 38%)

Overview

Miercom was engaged to validate Cisco CleanAir technology for interference classification, mitigation and avoidance, and to compare it with products from other vendors. The most up-to-date versions of wireless controllers and access points from Cisco, Aruba, Motorola, Trapeze, HP, and Meru were compared in terms of their respective performance for this evaluation.

We tested the impact of interference on throughput from a variety of non-Wi-Fi devices, including continuous wave type signals from video surveillance cameras, frequency hopping 2.4GHz and 5GHz phones and Bluetooth devices, and cyclic type from microwave ovens. The evaluation included the ability to detect and classify each type of interference from single sources and the ability to accurately classify multiple sources of interference. We also looked at the self-healing properties, i.e. the ability to identify major sources of interference, and switch to another channel to avoid them. Also included in the tests was examining the ability to detect an off-frequency rogue access point, hiding between standard Wi-Fi channels, that could provide backdoor access to the wired network.

Cisco CleanAir technology was able to detect interference sources, and identify and map the locations so that remediation actions can be taken.

WLAN Equipment Used:

Cisco Wireless LAN Controller 5508 (7.0.93.110)

 Cisco 3500-series 802.11n Access Point

Cisco Wireless Control System (7.0.130)

Cisco Mobility Services Engine 3350 (7.0.99)

Aruba 6000 controller with (3.4.2.2)

 Aruba AP125 802.11n Access Point

 Aruba AP105 802.11n Access Point

HP MSM760 controller with software (5.3.3)

 HP MSM422 802.11n Access Point

Motorola RFS7000 controller with software (4.2.1)

Motorola AP-7131N 802.11n Access Point with latest software (4.0.3)

Motorola AirDefense 1250 Services Console with latest software (8.0.0.15)

Motorola AirDefense M520 Sensor with latest firmware (5.2.0.11)

Trapeze MX-200R Controller (7.0.13.3)

 Trapeze MP-432 802.11n Access Point

Meru MC4100 Controller with software (3.6.1)

 Meru AP320 802.11n Access Point

802.11n clients (Intel 5300AGN – Driver 13.1.1.1)

Interference Sources:

Microwave Oven

Plantronics Bluetooth Wireless Headset

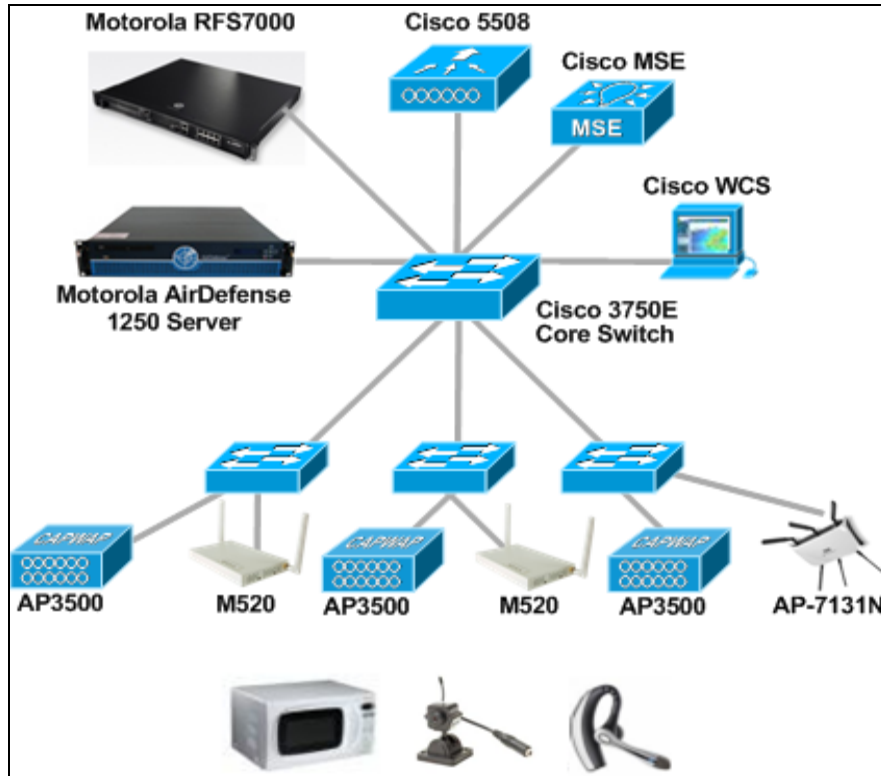
2.4GHz DECT Cordless Phone

5.8GHz DECT Cordless Phone

2.4GHz Q-See Wireless Video Surveillance Camera

5.8GHz Wireless Video Surveillance Camera (Model: W5803W1)

Test Bed Diagram



How We Did It

Classification test:

For Cisco, an environment was created which utilized three AP3500 series access points, the 5508 Wireless Controller, Cisco Wireless Control System (WCS), and Cisco Mobility Services Engine (MSE). For Motorola, we used two M520 sensors, one AP7131N access point, a Motorola AirDefense 1250 server, and Motorola RFS7000 WLAN controller. Sensor locations for both vendors were the same. Two sensors were placed at a distance of 50 feet apart, with the interference source located equidistant between them. The third sensor was located approximately 70 feet away. For interference sources, we used a standard countertop microwave oven, set for 2:00 minutes on HIGH during the test. We also used 2.4GHz and 5GHz cordless phone handset and base stations, 2.4GHz and 5GHz wireless video surveillance cameras, a Bluetooth headset and charging base station, as well as an RF jamming device.

Self-Healing test:

Five clients were placed at locations ranging from 10 to 100 feet from the access point. Each client was continuously receiving a looped low bandwidth video stream. Since the video player application performed buffering of the stream, we had a command prompt window continuously pinging the access point to determine the moment when communication was interrupted. Timing was performed with a stopwatch. We selected three locations for the interference source: Location A at 10 feet from the access point; Location B at 50 feet; and Location C at 100 feet. We expected each client to be affected at different levels based on their proximity to the interference source, and the interference source proximity to the access point. At location C, we expected that the client 100 feet away from the AP and closest to the interferer would be dropped, but others would continue to communicate in an unimpaired state. The interference source we chose was the 2.4GHz video surveillance camera, as it had the most negative impact, and the first AP we tested was the Cisco 3500 series.

Test Results

Impact of Interference

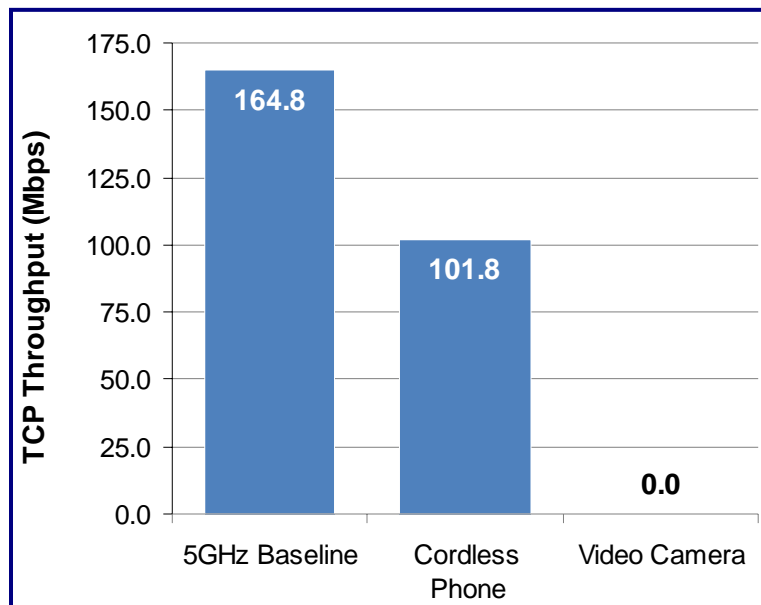
Tests were performed to determine what the impact was on performance from different types of non-Wi-Fi signals. The client was an 802.11n laptop and a Cisco 3500 served as the access point. Baseline throughput was measured in clean spectrum on a 40 MHz channel in the 5 GHz band. Individual interference signals were turned on and the throughput measurement was taken. Multiple runs were performed to obtain an average. Baseline throughput was 164.8 Mbps on the clean spectrum.

When a 5GHz wireless video surveillance camera was activated, Channel 153 was jammed with continuous wave interference and the client was knocked off the air. Network throughput was 0% while the video camera was operating.

We used 5GHz DECT to record the signaling impact of frequency hopping. We used three phones: two were conferenced, and one was the base station connected to a landline. With three phones in use, network throughput dropped to 102 Mbps, and the AP measured an air quality of 86% out of a 100% for the 5GHz.

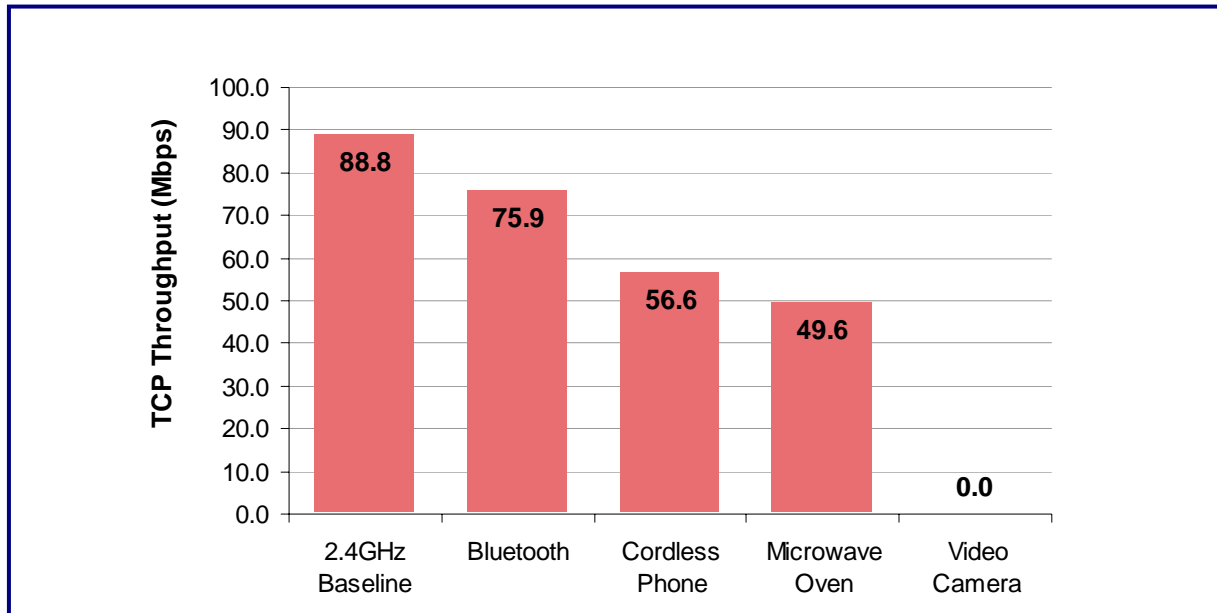
See [Figure 1](#) for the 5.0GHz baseline values.

Figure 1: 5.0GHz Baseline Measurements with Impact of Interference on Throughput



Baseline measurement comparison with Cordless Phone and Video Camera

Figure 2: 2.4GHz Baseline Measurement with Impact of Interference on Throughput



Comparing the baseline with interference from Bluetooth, Cordless Phone, Microwave and Video Camera. Each non-Wi-Fi interferer has different effects and was tested individually and compared to the baseline.

Interference on the 2.4GHz Wi-Fi band was then tested. This band consists of channels 1, 6 and 11. The baseline on a clean spectrum was 88.849 Mbps. When a Bluetooth headset was active, transmitting voice, throughput dropped to 76 Mbps. Bluetooth is also a frequency hopping type of interference.

We used 2.4GHz cordless phones to record the signaling impact of frequency hopping. We used three phones: two were conferenced, and one was the base station connected to a landline. With three phones in use, network throughput dropped to 57 Mbps.

Cyclic type of interference is created by microwave ovens and affects channels in the upper portion of 2.4GHz including 6 through 11 depending on the model. With the oven set for two minutes on high power, network throughput was reduced to 50 Mbps. See [Figure 2](#) for the 2.4GHz baseline values.

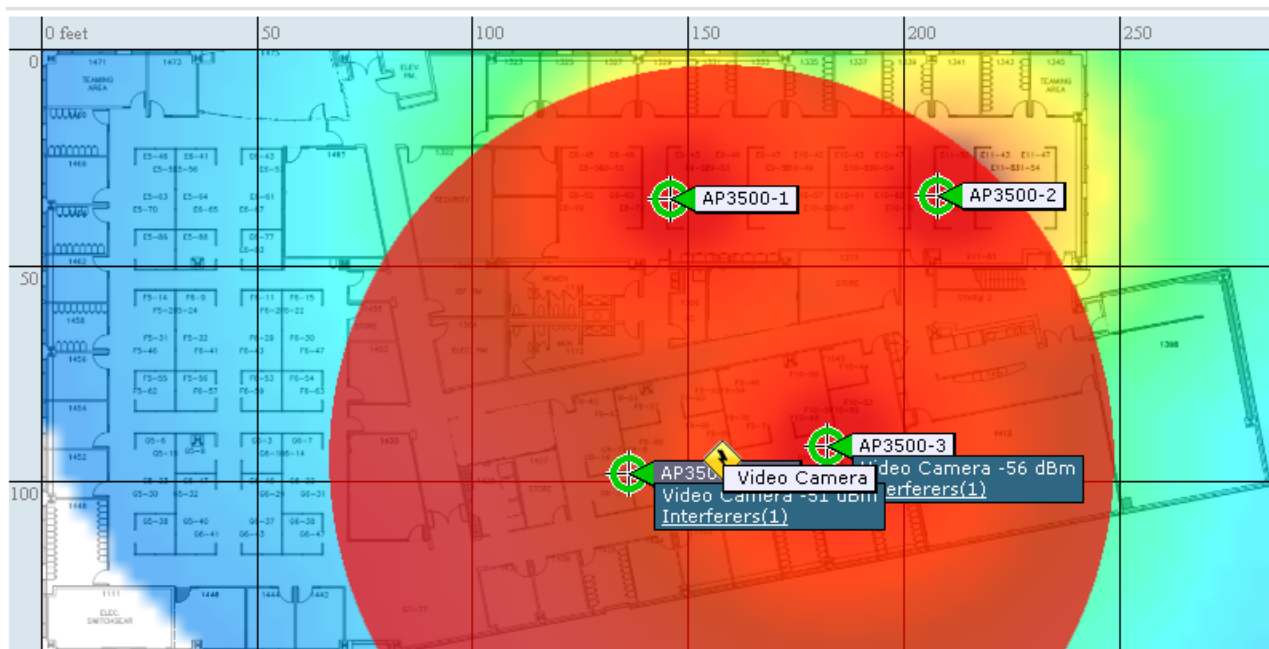
When a 2.4GHz band wireless video surveillance camera was engaged, 0 Mbps throughput was noted.

Interference Classification

In addition to knowing the impact that other signaling devices have on a network, we need to identify the location and source in order to remediate the problem. We evaluated Cisco CleanAir technology with the Aironet 3500 Series and the Motorola AirDefense solution with the AP-7131N access point and the M520 sensor. Both solutions classify sources of interference whereas other vendors tested do not offer interference classification capabilities.

The Cisco Aironet 3500 Series access point has a built-in spectrum analyzer from a new custom CleanAir ASIC in the AP which allows real-time network monitoring while providing WLAN services to clients. The Motorola AP-7131N also provides spectrum analysis. The AP can provide either WLAN services or can monitor the spectrum, but not both simultaneously. Disabling an access point to provide interference monitoring can increase the load on other APs and reduces network capacity. Since it is a standard Wi-Fi chipset, the resolution of its analysis is limited. We observed a scanning resolution of 78 KHz for the Cisco CleanAir, and 5 MHz for the Motorola. This offers as much as 64x the scanning resolution compared to Motorola.

Cisco CleanAir also provides mapping via the WCS UI which allows it to pinpoint the physical location of an interfering signal.



This is a screen shot of the Cisco WCS displaying the physical location of a video camera interference source. The red circle centered around the device represents the interferer's zone of impact.

We tested using single interferers and multiple interferers in the 2.4GHz band, and single interferers in the 5GHz band.

Screen shot from Cisco

Worst 802.11b/g/n Interferers *								
Interferer ID	Type	Status	Severity	Affected Channels	Duty Cycle (%)	Discovered	Last Updated	Floor
a8:09:7e:00:00:1b	Video Camera	Active	97	1..5	100	Tue Mar 30 13:49:44 PDT 2010	Tue Mar 30 13:51:35 PDT 2010	System Campus > MR-1 > MR1-Floor1
a8:09:7e:00:00:20	Microwave Oven	Active	27	6..11	17	Tue Mar 30 13:51:22 PDT 2010	Tue Mar 30 13:52:13 PDT 2010	System Campus > MR-1 > MR1-Floor1
a8:09:7e:00:00:1d	DECT Like Phone	Active	4	4..11	8	Tue Mar 30 13:50:15 PDT 2010	Tue Mar 30 13:51:21 PDT 2010	System Campus > MR-1 > MR1-Floor1
a8:09:7e:00:00:1e	Bluetooth Link	Active	3	3..11	6	Tue Mar 30 13:50:16 PDT 2010	Tue Mar 30 13:51:01 PDT 2010	System Campus > MR-1 > MR1-Floor1
a8:09:7e:00:00:1c	DECT Like Phone	Active	2	2..11	2	Tue Mar 30 13:50:06 PDT 2010	Tue Mar 30 13:51:15 PDT 2010	System Campus > MR-1 > MR1-Floor1

This picture shows the successful classification of multiple simultaneous interference sources.

We began with a single 2.4GHz video surveillance camera as our source of interference. Motorola triggered an alarm for a “continuous wave” but could not identify the device. The Cisco WCS identified the device as a video camera, located it and indicated that the interference severity was 98. The Cisco wireless controller UI also displayed the Wi-Fi channel utilization and air quality as poor.

With the microwave oven test, Motorola provided two alarms, one at the access point and one at the sensor, and correctly identified the source. The access point detected the interference at 2437MHz, while the sensor detected interference at 2462MHz. No correlation is provided by Motorola so the same device showed up as two alarms within the AirDefense system.

Cisco detected and identified the interference as a microwave oven from three access points and reported a single event. It detected which channels were affected, and located the oven. This information remains available after the interference has passed, for remediation of periodic interferences.

A DECT cordless phone base station was placed in the environment. The base station produces interference when it tries to communicate with the handsets, but it is at a lower duty cycle than an active call. Motorola displayed the interference on the spectrum analysis UI, but could not identify the source. The low duty cycle was not enough for it to identify. Cisco classified the source as a “DECT-like phone,” and pinpointed the physical location.

The duty cycle was increased by adding an active handset to our base station. This time, Motorola detected the interference at the access point, as well as two sensors, and identified the source as a “frequency hopper.” Detection was intermittent. Cisco detected and classified the phone and base station as “DECT-like phone,” and again mapped the physical location.

We added two more handsets and made them all active. Motorola classified the source of interference as a frequency hopper. Detection remained intermittent. We tested the Motorola using both the Full Scan mode and Interference Scan mode. Detection was intermittent for both

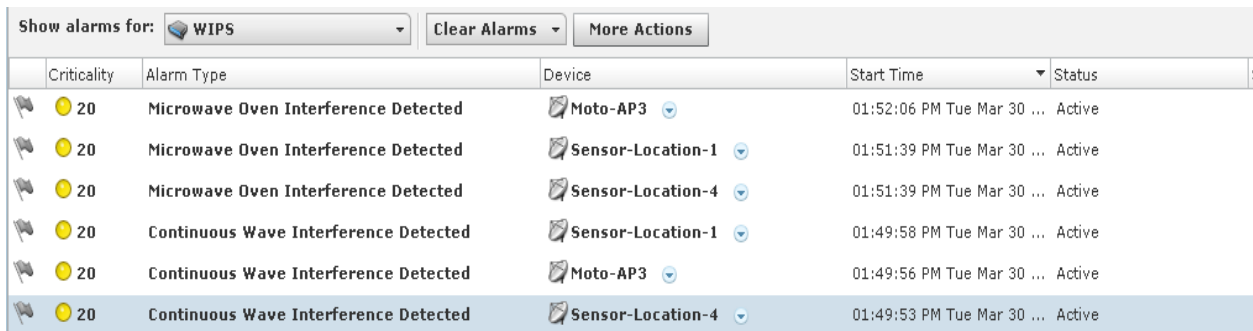
modes; in Interference Scan mode, the closest AP to the source did not detect, and the two sensors misclassified the source as Bluetooth.

Cisco correctly classified and mapped the physical locations of each phone in relation to the access points.

Bluetooth is low duty cycle - 1% interference - when in Discovery mode. A Bluetooth headset was put into the test environment to ascertain if Cisco or Motorola could detect it. Neither Cisco nor Motorola were able to detect the device since Bluetooth discovery only occurs for a very brief period of time. With the Bluetooth headset active, the duty cycle was 15%. Motorola detected the interference intermittently on one sensor, but not on the access point closest to the interference source. Since Motorola does not assign a unique ID to each interferer, it was listed as the misclassified Bluetooth from the previous cordless phone test. The alarm showed the start time from the previous test, but not when it ended. The Bluetooth alarm was also assigned the same severity level as continuous wave, even though the real-world impact of these two types of interference are different.

Cisco detected and correctly classified this Bluetooth device as a unique interferer, displayed the location on a floor plan of the environment, and displayed the severity.

Screen shot from Motorola



The screenshot shows a web interface for WIPS (Wireless Intrusion Prevention System) alarms. At the top, there is a dropdown menu set to 'WIPS', a 'Clear Alarms' button, and a 'More Actions' button. Below this is a table with the following columns: Criticality, Alarm Type, Device, Start Time, and Status. The table contains six rows of data, all with a criticality of 20 and a status of 'Active'. The alarm types are 'Microwave Oven Interference Detected' and 'Continuous Wave Interference Detected'. The devices listed are 'Moto-AP3', 'Sensor-Location-1', and 'Sensor-Location-4'. The start times range from 01:49:53 PM to 01:52:06 PM on Tuesday, March 30.

Criticality	Alarm Type	Device	Start Time	Status
20	Microwave Oven Interference Detected	Moto-AP3	01:52:06 PM Tue Mar 30 ...	Active
20	Microwave Oven Interference Detected	Sensor-Location-1	01:51:39 PM Tue Mar 30 ...	Active
20	Microwave Oven Interference Detected	Sensor-Location-4	01:51:39 PM Tue Mar 30 ...	Active
20	Continuous Wave Interference Detected	Sensor-Location-1	01:49:58 PM Tue Mar 30 ...	Active
20	Continuous Wave Interference Detected	Moto-AP3	01:49:56 PM Tue Mar 30 ...	Active
20	Continuous Wave Interference Detected	Sensor-Location-4	01:49:53 PM Tue Mar 30 ...	Active

In the test case using multiple simultaneous interference sources, Motorola did detect the microwave oven and the video camera but it missed the DECT phone and Bluetooth sources, which are both frequency hoppers. Note that multiple alarms were triggered even though only one microwave was on.

Multiple Sources of Interference – 2.4GHz Band

We wanted to determine if CleanAir and AirDefense could correctly classify multiple interferers if operating simultaneously.

We used two video surveillance cameras, one on Channel 1, and the other on Channel 11. Cisco correctly classified both sources of interference as video cameras, reporting that one was affecting channels 1-4, and the second affecting channels 9-11. It also displayed the physical location on the floor plan.

Motorola triggered alarms on both sensors and on the access point but was unable to determine if one device or multiple devices were causing the alarms. Each sensor and the access point showed a single interference alarm.

We then added additional interferers. The multiple interference sources consisted of a 2.4GHz DECT phone, a 2.4GHz video camera, a Bluetooth headset, and a microwave oven.

Cisco detected, classified, and located all devices accurately. The microwave oven location icon was initially hidden by the video camera location icon.

Motorola detected and set an alarm for a continuous wave device (the video camera) at 2462MHz, and also correctly classified the microwave oven, but was unable to detect the DECT phone or the Bluetooth headset as frequency hopping devices.

Single Interferers – 5GHz Band

We also examined each product's ability to classify single interference sources in the 5GHz band.

Beginning with the DECT cordless phone, Cisco was able to detect and properly classify and locate the device as a "DECT-like phone."

As previously shown in the 2.4GHz testing, the low duty cycle hampered Motorola to detect and it did not trigger any alarms.

To increase duty cycle of the interference, we added a handset and made it active. Cisco again correctly classified and mapped the location of the phone. Motorola intermittently detected and set alarms for a frequency hopper on one sensor only, but not on the access point.

With three phones active, the Motorola AP and both sensors detected and set alarms for a frequency hopper. Cisco classified and located all three phones correctly.

We then placed a 5GHz video camera into the environment. Motorola was unable to detect or identify the interference, possibly because the duty cycle of the interference was insufficient to cross the threshold to trigger an alarm. Cisco was able to classify and locate the video camera accurately.

A summary of the interference source and how it was detected and classified is shown in [Figure 3](#) on page 13.

Figure 3: Classification and Information on Interferers by Cisco CleanAir and Motorola AirDefense

Interference Source		Classified?		Motorola AirDefense Notes
Frequency Band	Type	Cisco Clean Air	Motorola AirDefense	
2.4GHz	Video Camera	Yes	Yes	Classified generically as a "Continuous Wave"
	Microwave Oven	Yes	Yes	Two alarms displayed - one for each sensor, no correlation.
	DECT Base station only	Yes	No	Motorola needs to see a high duty cycle to classify.
	DECT Base Station + One Phone	Yes	Intermittent	Motorola will classify - but it is intermittent.
	DECT Base Station + Three Phones	Yes	Misclassified	One sensor did not detect it. Other sensors fired both a Bluetooth & Frequency hopper alarm
	Bluetooth	Yes	Intermittent	Intermittent and only detected on one sensor
	Jammer	Yes	Misclassified	Motorola misclassified it as a Microwave for 1 second
Multiple 2.4GHz	Video Camera (Ch1) Video Camera (Ch11)	Yes	No	Motorola provided an alert of "Continuous Wave" on all sensors - but did not list two devices as the cause.
	DECT Phone, Video Camera, Bluetooth, Microwave	Yes	No	Only Microwave and Video Camera identified
5GHz	DECT Base Station	Yes	No	Motorola needs to see a higher duty cycle to classify.
	DECT Base Station + One Phone	Yes	Intermittent	Intermittent and only detected on one sensor
	DECT Base Station + Three Phones	Yes	Yes	
	Video Camera	Yes	No	

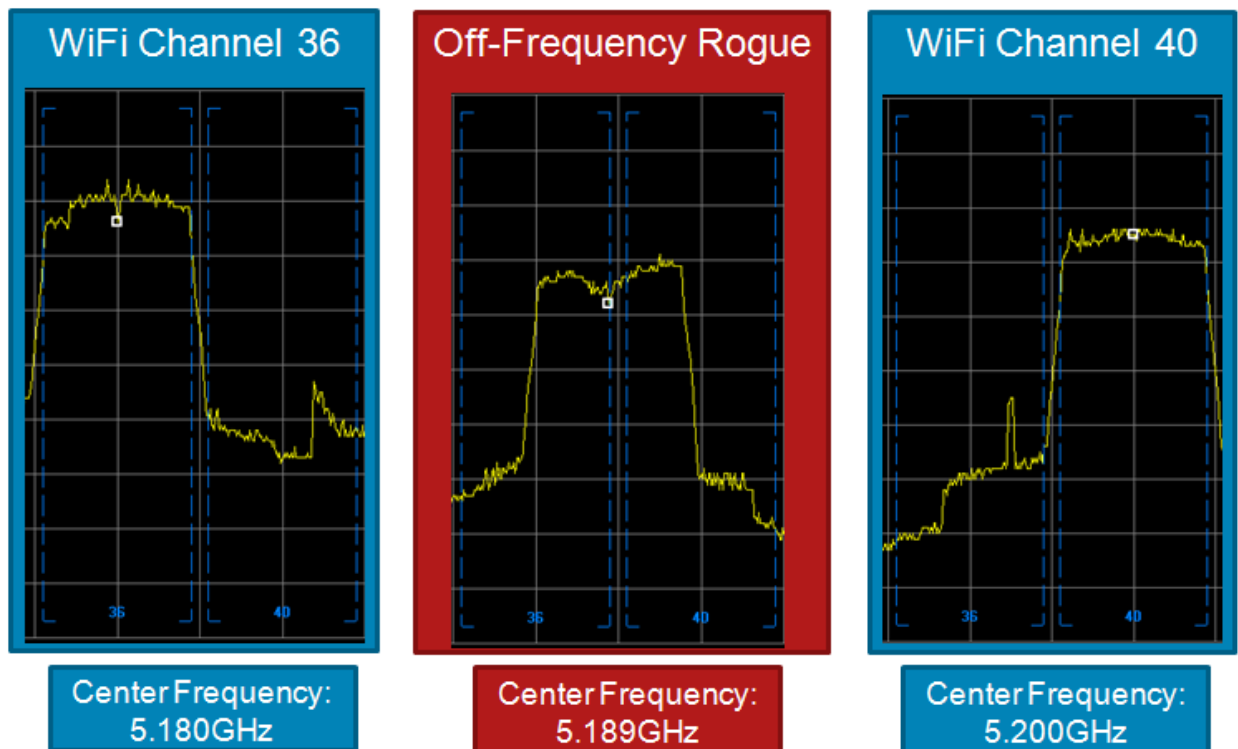
Rogue Devices on Non-Standard Channels

Because rogue devices can compromise the wired network by allowing “back door” access, the access points were tested to see if they would detect such a threat.

We configured a Cisco AP as a workgroup bridge and placed it on Channel 36. We gave this bridge an SSID of “Stealth” and then checked to see if it was detected.

Cisco correctly identified the bridge as a rogue AP. Trapeze also correctly identified the rogue. Motorola detected it as an “Unsanctioned BSS.” HP also detected it as a rogue and Aruba detected the SSID of “Stealth.” Meru did not detect the rogue.

Virtually all APs were able to detect a rogue device placed in the network. We then wanted to test what would happen if a rogue is configured off-channel. There are products available which enable users to alter the center frequency of Atheros-based chipsets that are used in the majority of Wi-Fi access points, and thereby hide them from the network. To determine if this type of off-frequency rogue could be detected, the center frequency of our rogue was altered to 5.189GHz. We reran the test after placing it between channels 36 and 40.



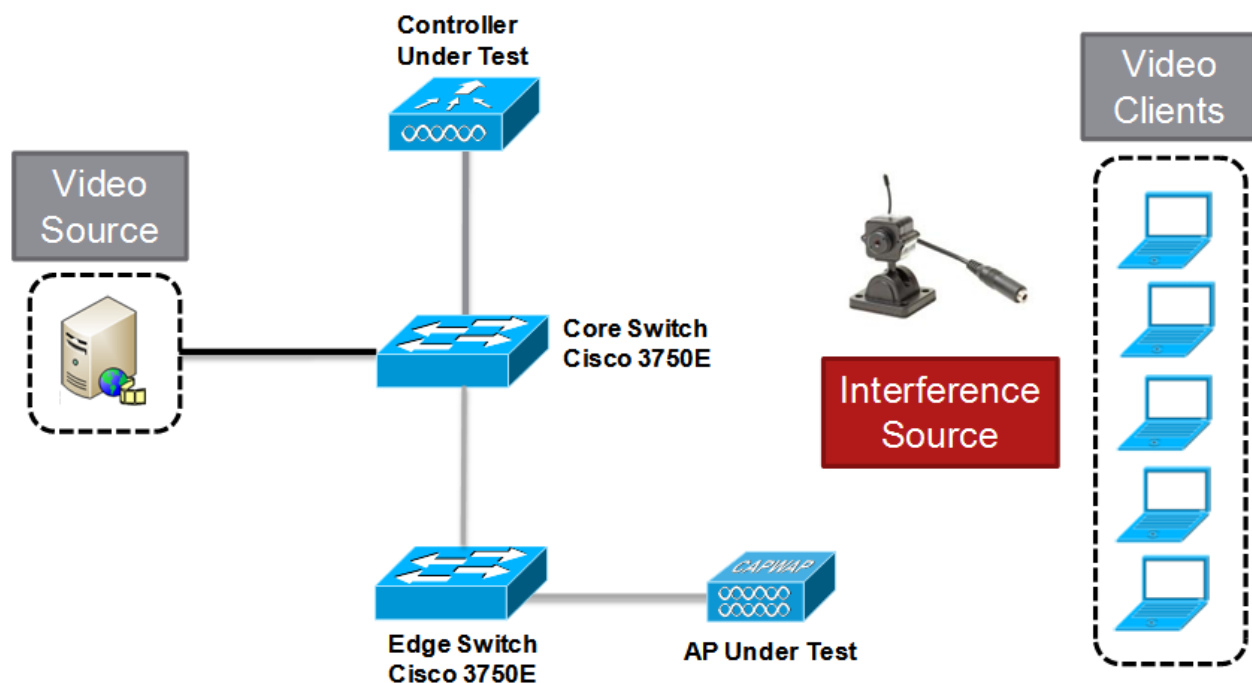
Cisco was able to correctly identify the rogue as “Wi-Fi invalid channel” and mapped its location. All other vendors scanned for off-channels, but not off-frequencies. Aruba was unable to detect the rogue at its new frequency, as were Trapeze, Motorola, HP and Meru.

Self-Healing

Given the negative impact of non-Wi-Fi interference on a wireless network, access points need to avoid this interference to protect the end user Quality of Experience (QoE). We conducted this test using the 2.4GHz band.

Cisco Equipment:

With the camera enabled in Location A, all five clients immediately lost ping. The access point switched from Channel 1 to Channel 6, and clients recovered ping in 49 seconds. When the camera was engaged at Location B, the AP took 39 seconds to change channel and client to recover ping. With the camera in Location C, the access point took 1:04 to change channel and recover ping. As the Cisco AP has persistent avoidance, we reset the access point between tests to clear it so that alternate channels would not get locked out by the feature. In normal operations, persistent device avoidance automatically ages out the interference source to make the channel available to the system once again. A second run at each location took 30 seconds at Location A, 41 seconds at Location B, and 48 seconds at Location C. As expected at the 100 feet location, only the farthest client was failing ping. Although video quality was impacted on all clients, the access point detected interference and changed channels.



Aruba Equipment:

The same test was run on the Aruba AP125. With the camera in Location A, Aruba reported a noise level of -87dBm while a spectrum analyzer reported the noise level at -52dBm. As the channel was completely jammed, no errors were reported. Since the noise level and error thresholds were not crossed, the access point did not change channels and all clients were disconnected.

With the camera in Location B, clients far from the access point were affected and near clients were not affected due to the signal-to-noise ratio. The noise level threshold was triggered, and the access point changed channels in 2:01 minutes.

At 100 feet, the noise level read -75 to -77dBm and was not high enough to trigger. Clients far from the AP were affected most, and high latency and degraded bandwidth was experienced for

the whole cell. A second test run never changed channel at 10 feet, took 2:10 to change at 50 feet, and 2:22 to change at 100 feet when a noise level of -70dBm triggered the threshold.

The Aruba AP105 was also evaluated for its self-healing capability. The baseline noise level read -105dBm. This reading was too low, and did not agree with the reading of the AP125 in the same environment, which read -87dBm. In a network environment containing both AP105 and AP125 devices, this mismatch in noise floor readings made it difficult to adjust the noise threshold necessary to change channels. The noise level must be above the threshold for 120 seconds in order for a channel change to be triggered. After 30 minutes of lost clients due to the video camera interference at the 10 feet location, the inaccuracy observed proved that the noise level never remained above the threshold long enough to set the trigger. It was also observed via the CLI interface that the AP kept resetting the radio.

In the 50 feet location, all clients lost ping when the camera was turned on. The AP105 reported a noise level of -74 to -80dBm, but did not change channels over the 30 minute test duration.

At 100 feet, all clients lost ping when the video camera was engaged. The noise reading on the AP was -100dBm, and after 30 minutes of dropped clients, no channel change was observed. We tried raising the setting for "Non 802.11 Interference Immunity" to Level 5 from the default of Level 2, but all five clients remained unable to ping the access point.

HP Equipment:

The smallest channel change interval for the HP access point is one hour. When the video camera was turned on at 10 feet, the AP lost all clients. After more than an hour later, the AP had not changed channel, nor logged anything in the event log. At 50 feet, only one client that was closest to the AP remained on after the camera was turned on. Over one hour later, HP did not change channel or log any events. At 100 feet, four clients remained connected, and only the farthest client was jammed, as expected. Over one hour later, the AP had not changed channel.

Trapeze Equipment:

Trapeze has a default scan interval of 3600 seconds, and the minimum scan time can be set to 900 seconds. With the video camera at 10 feet away, all clients dropped and Trapeze changed channels after 47 minutes. At 50 feet, one client remained connected. After over an hour later, Trapeze did not change channel. We noted that the noise level always reported -96dBm, regardless of the position or distance of the jamming interference from the video camera. At 100 feet, only the farthest client was affected. After over an hour, Trapeze did not change channels.

Motorola Equipment:

Motorola AP-7131N offers legacy self-healing as well as the feature, Smart-RF. We enabled Auto Channel Select and modified the data rate settings on the AP to increase available bandwidth, and reduce channel utilization to support the video stream used in our testing.

With legacy self-healing, the AP uses the average number of retries as a trigger threshold to change channels. With the video camera in the 10 feet location, Motorola reported 0 retries. It could not detect any interference. The client throughput was low enough that it was represented in scientific notation. After one half hour, the access point had not changed channels. The Smart-RF feature was enabled and retested, but the same results were seen. No retries were seen, and no noise level was reported. All statistics were zeroed out. The network was completely jammed, but the access point could not detect it, and did not change channels.

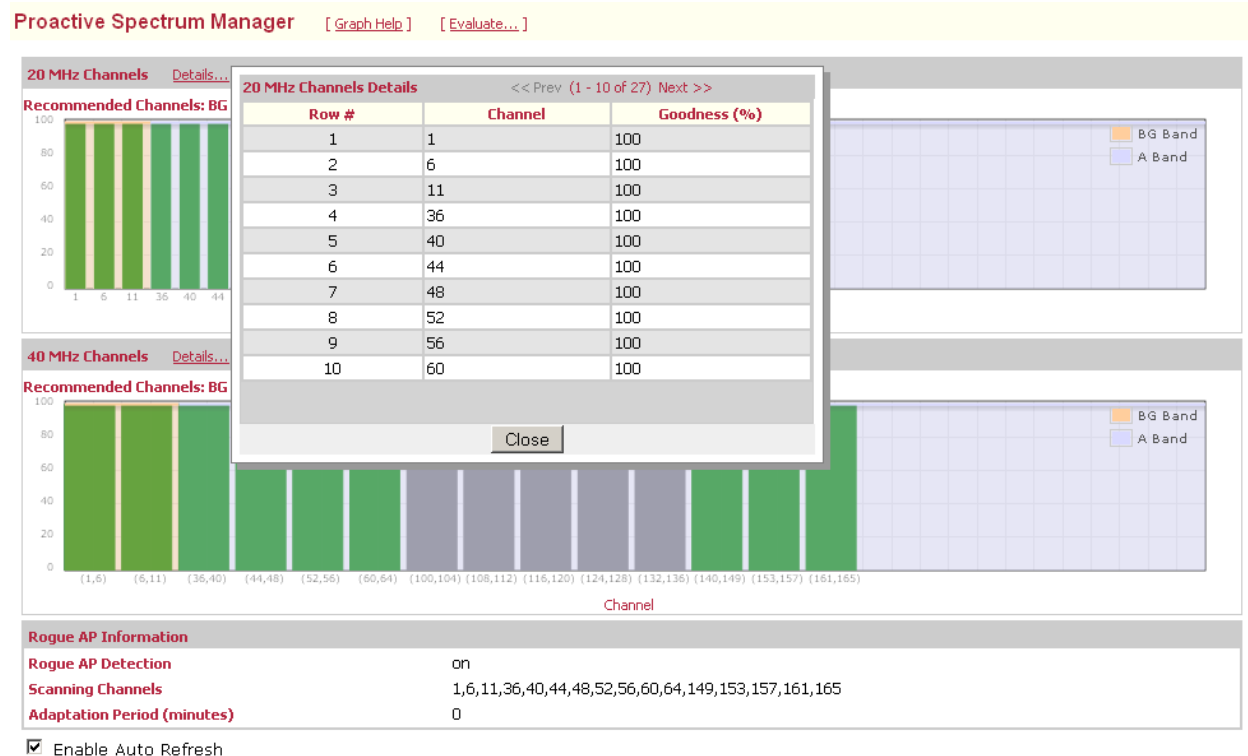
At 50 feet, the average number of retries hovers between 1 and 2, and does not trigger the threshold. After 20 minutes, the channel had not changed and we attempted to force ACS to execute a channel change, but it did not occur.

With the video camera at 100 feet from the access point, only the farthest client was affected. Noise level reading was -66dBm. After one half hour, the access point did not change channels. Our attempt to force ACS to switch channels manually was unsuccessful.

Meru Equipment:

Meru’s AP320 uses the Proactive Spectrum Manager feature. It displays the level of “goodness” of each channel. When we sent video streams over a clean channel, PSM reported the channel as “bad” due to the high utilization, but when the channel was jammed by the video camera, resulting in no utilization, PSM reported a 100% “goodness” score for the channel.

This 802.11n access point essentially does not support auto channel as the 802.11 a/b/g models do, nor does it appear to support self-healing. PSM does evaluate the channel every user-defined number of seconds, and then moves stations to a clear channel. The only threshold which is used to trigger this change is the presence of rogues.



Screenshot taken while the video camera was completely jamming the channel. Meru reports a 100% “goodness” score for the channel, because the jamming interference means that Wi-Fi channel utilization is in fact 0%, from Meru rating of channel quality. Meru would not change channels even if the channel is completely jammed and unusable by Wi-Fi.

We measured the relative noise levels on the Meru access point to determine their accuracy. Meru measured a noise level of -82dBm as a baseline on a clean channel. With our video camera 50 feet away, the noise floor read -85dBm. With the video camera at a distance of 100 feet, the noise floor reading was -71dBm. See [Figure 4](#) on page 18 for a summary of the results.

Figure 4: Summary of Self-Healing Tests between Cisco CleanAir and Other Competitors

Interferer Distance from AP	Time to Self-Heal						
	Cisco	Aruba AP 125	Aruba AP105	Motorola	HP	Trapeze	Meru
Close (10ft)	30 sec	Never	Never	Never	Never	47 min	Never
Medium (50ft)	41 sec	2:10	Never	Never	Never	Never	Never
Far (100ft)	48 sec	2:22	Never	Never	Never	Never	Never
Notes:		At the close location, noise remained at -87dBm	Noise varied at each location but never remained above the change threshold.	The number of retries did not cross the threshold to trigger a change.	HP saw a noise level of -70dBm when camera was at 50ft.	Noise level remained at -96dBm.	Channel "Goodness" always remained at 100%.