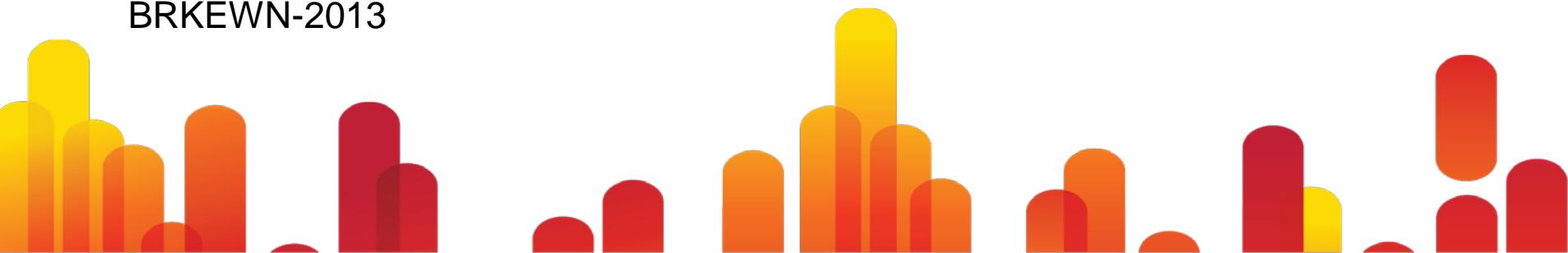




Cisco *live!*

Understanding CleanAir Technology to Improve Wlan Spectrum Management

BRKEWN-2013



Housekeeping

- We value your feedback- don't forget to complete your online session evaluations after each session & complete the Overall Conference Evaluation which will be available online from Thursday
- Visit the World of Solutions
- Please remember this is a 'non-smoking' venue!
- Please switch off your mobile phones
- Please make use of the recycling bins provided
- Please remember to wear your badge at all times

Agenda

- Why does interference matter?
- CSMA-CA and Duty Cycle?
- AP modes of Operation
- Technical Details
 - Interference Detection
 - Interference Mitigation
 - CleanAir Monitoring
 - Spectrum Expert Mode
- Configuration Essentials

RF terms and Wi-Fi behavior basics



The Impact of a Crowded Spectrum Performance At Risk in Unprotected Networks



End User Impact

- Reduced network capacity and coverage
- Poor quality voice and video
- Potential complete link failure

IT Manager Impact

- Potential security breaches
- Support calls
- Increased cost of operation

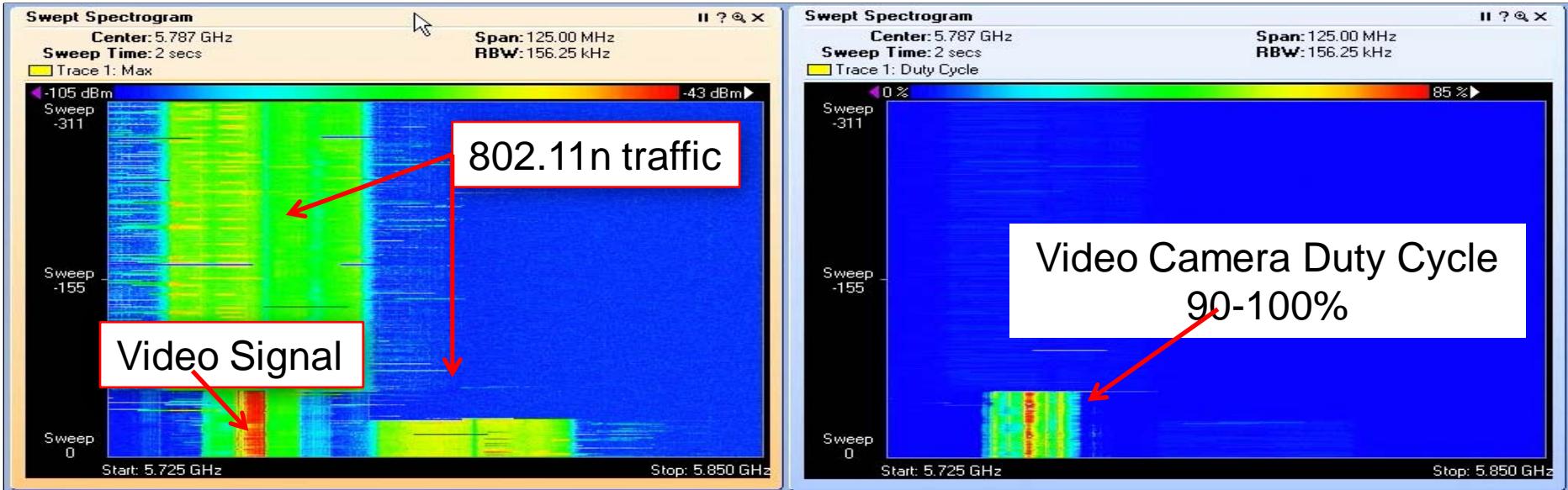
Interference Type	Throughput Reduction	
	Near (25 ft)	Far (75 ft)
2.4 or 5 GHz Cordless Phones	 100%	100%
Video Camera	 100%	57%
Wi-Fi (busy neighbor)	 90%	75%
Microwave Oven	 63%	53%
Bluetooth Headset	 20%	17%
DECT Phone	 18%	10%

Source: FarPoint Group

How does Interference impact Wi-Fi? Separating the FUD from the Fact's

- 802.11a/b/g/n - CSMA/CA or LBT (listen Before Talk)
- Collision Avoidance – 802.11 very very polite – by design
 - CCA
 - Collisions
 - SNR
- CCA – Clear Channel Assessment
 - ED – quick – low power - prone to false positives
 - Preamble – takes time – power – less prone to false
- CCA threshold for 802.11b/g is -65 dBm
- CCA for 802.11a is different -65 dBm ED, if true then 20 dB lower for Preamble interrogation needs to be processed -85 dBm

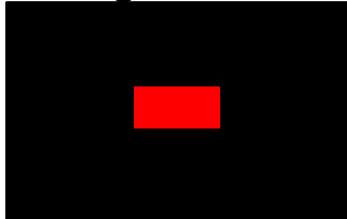
CCA Blocked or High



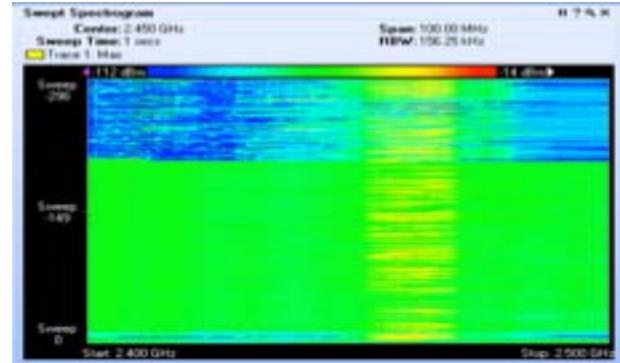
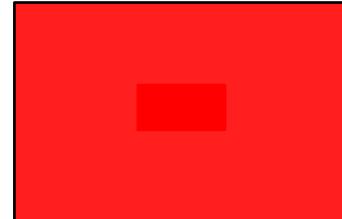
How does Interference impact Wi-Fi? Separating the FUD from the Fact's

- Collisions - Non Wi-Fi devices do not participate in our CA mechanism – they have their own
- No respect for Wi-Fi – results in:
 - Corrupted packets
 - Increased retransmissions
 - Increased Duty Cycle
 - Less available bandwidth
- SNR – Signal to Noise ratio

High SNR



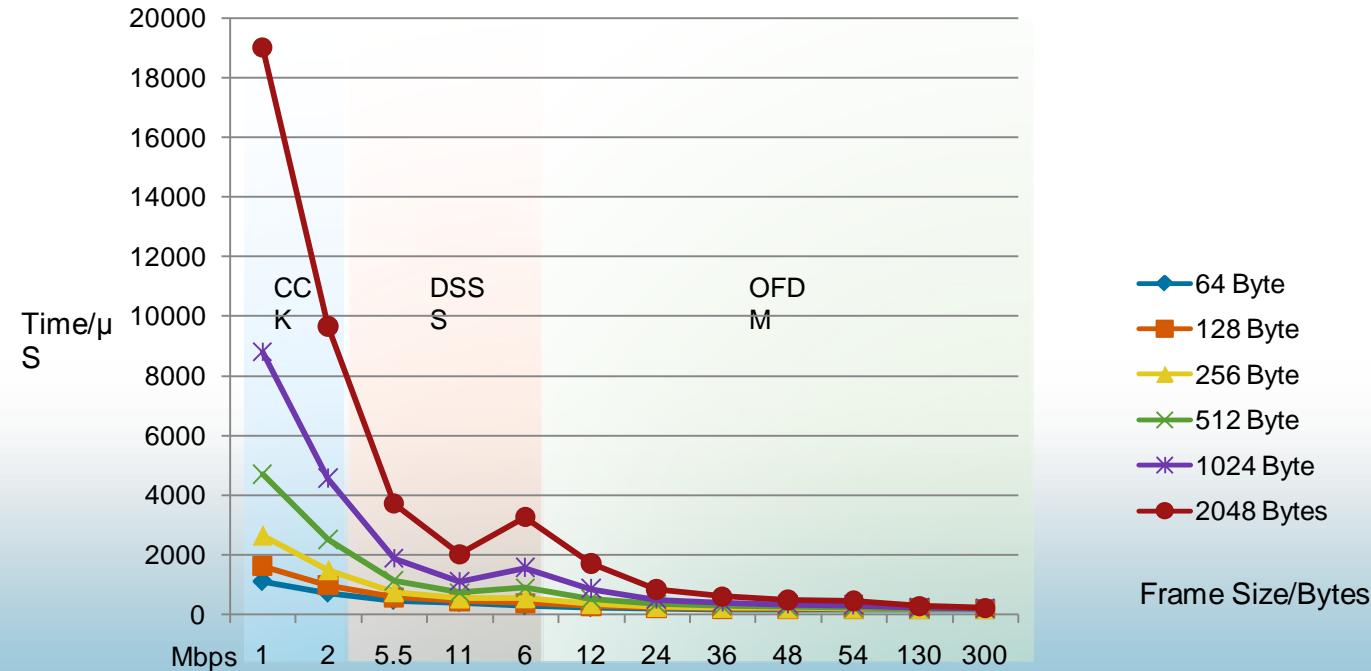
Low SNR



802.11 and Duty Cycle – Channel Utilization

- Retransmit a packet
- Duty Cycle of interference is directly proportionate to channel time available
- Busy network – less interference tolerance
- Less busy – might not even notice low levels of interference
- Bandwidth is like Money – the more you get the more you spend

Understand Protocol Selection 802.11 b/g/a/n and Duty Cycle—Important? Why?



Frame Size/Bytes

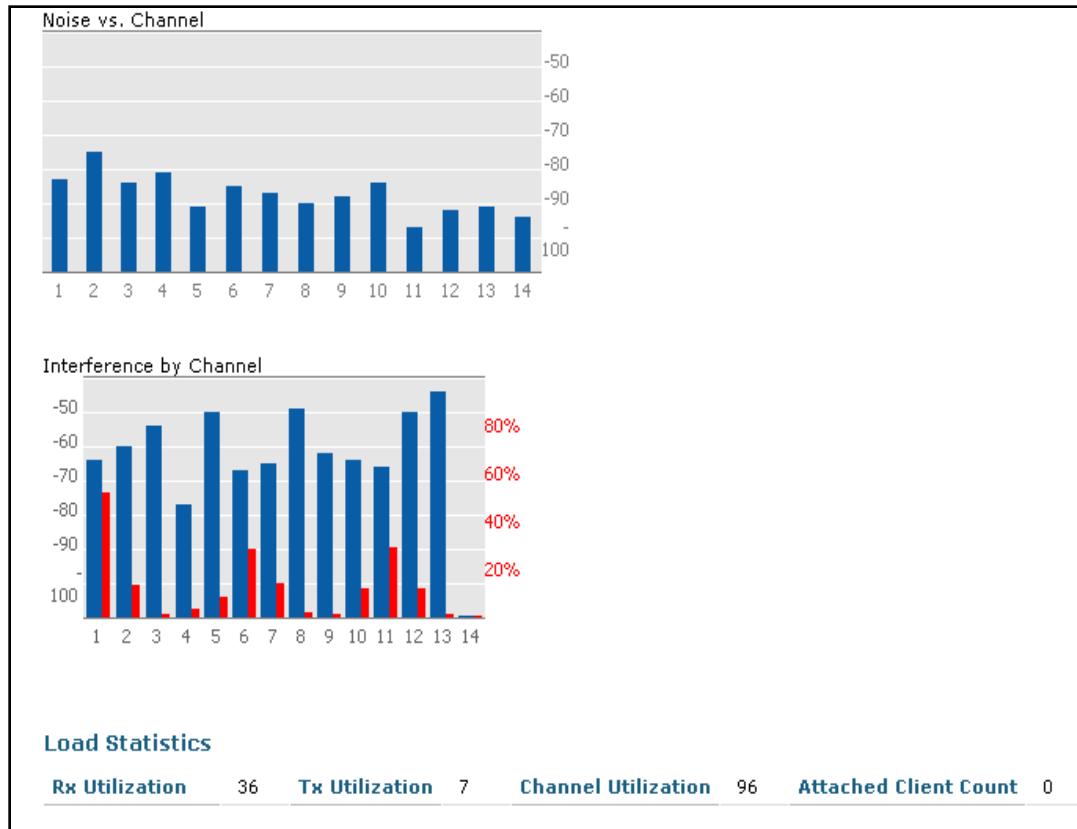
- 64 Byte
- 128 Byte
- 256 Byte
- 512 Byte
- 1024 Byte
- 2048 Bytes

Spectrum is a Shared Finite Resource

Cisco Access Points – Modes of Operation



Any Cisco Access point already sees and reports noise and interference per Channel



Wi-Fi and Spectrum Knowledge – Why is silicon important?

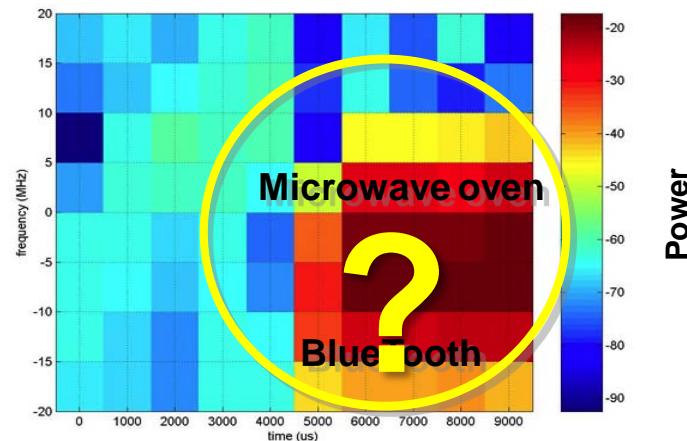
- A Wi-Fi chip is a communications processor – a MODEM
- It only knows
 - Energy that can be demodulated = Wi-Fi
 - Energy that can not be demodulated = Noise
- Noise is complicated –
 - Collisions, fragments, corruption
 - Wi-Fi that is below sensitivity threshold of the receiver
- Peaks in Wi-Fi activity can cause all of the above to occur

High Resolution Spectral Advantage

The Industry's ONLY in-line high-resolution spectrum analyzer

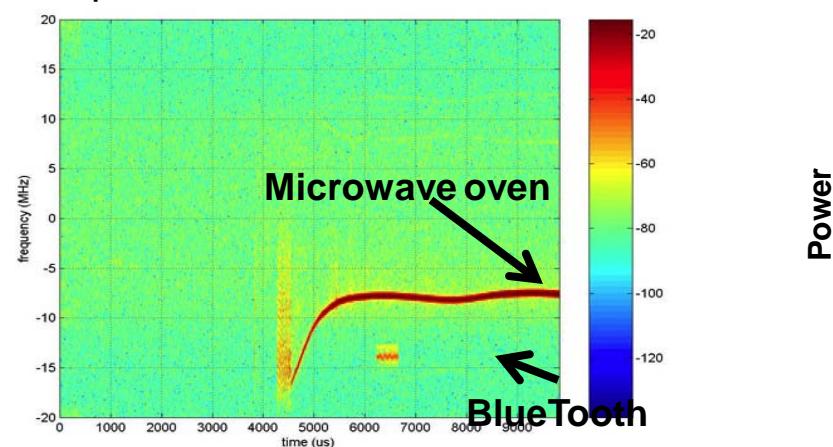
Typical Wi-Fi chipset

Spectral Resolution at 5 MHz



Cisco CleanAir Wi-Fi chipset

Spectral Resolution at 78 to 156 KHz



'Chip View Visualization' of Microwave oven and BlueTooth Interference

The Value of ASIC Based Intelligence

Troubleshooting Workflow	Response A: CleanAir Technology	Response B: Software-only Solution
Event: SpyCam and Microwave causing strong interference		
Detect presence of interference	Two unique sources detected by all APs	Energy detected by all APs
Classify source of interference	Spycam and microwave uniquely identified	Inability to differentiate between multiple sources of interference
Correlate interference events across APs	Interference correlated across all APs as two events	None – seen as unique event by each AP
Assess impact to AP and network	Severity and impact of each interferer measured	Total Interference measured only
Alert to IT	Intelligent alert on sources and impact	One alert per AP on “interference detect”
Physically locate SpyCam and Microwave	Interferers precisely located on floor map	Unable to locate automatically, manual search for both
Mitigate impact of interference	Intelligent and automatic channel change	Manual changes based on limited data
Air Quality Report	Network-wide view of Wi-Fi health by AP	None

Enterprise Wireless Evolution

From Best Effort to Mission Critical

2005

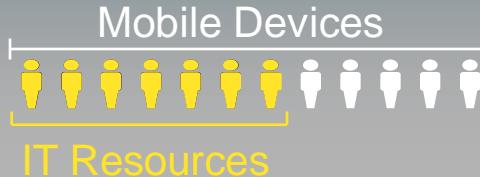
2011



Market Transitions

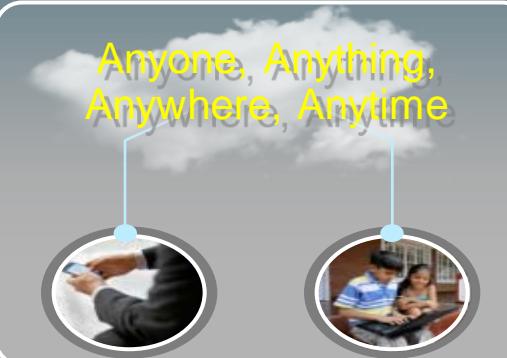
Mobility

1.3 Billion new Networked Mobile Devices in the Next Three Years



Workplace Experience

Blurring the Borders:
Consumer ↔ Workforce
Employee ↔ Partner



Video

50% of all Cisco Network Traffic Today Is Video



“When the students returned this year, if you asked me what percentage of students are using the Wi-Fi network – I would have told you 40%. I was shocked to see 85% of them using the Wi-Fi network”

Scott Ksander – September 2009 – Cisco Education TAB
Purdue University



Influx of Mobile Devices Creates IT Challenge

IT Consumerization: Now a Reality

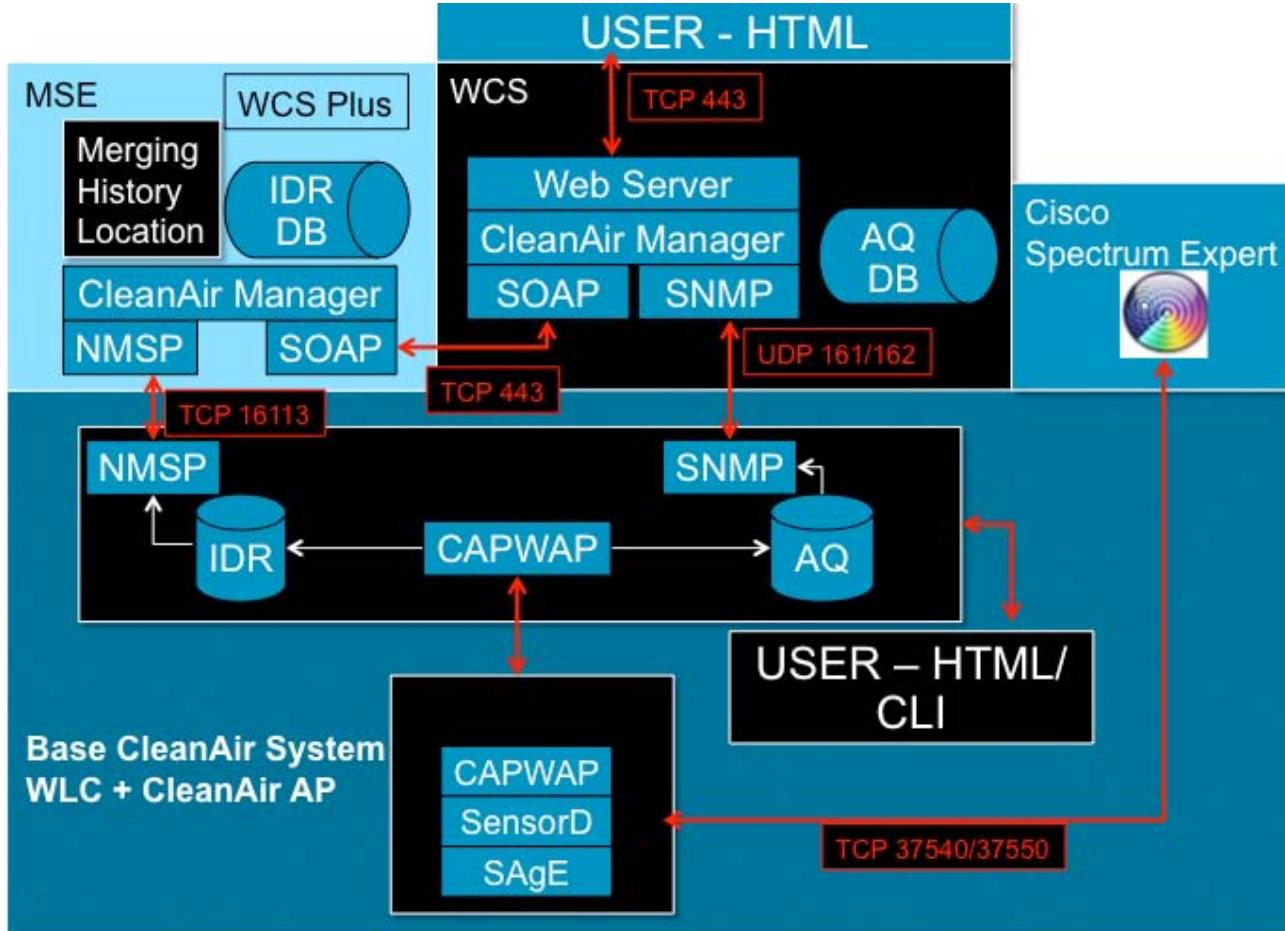
Smartphone adoption is growing at 50%+ annually

A Smartphone can use as much bandwidth as 200 legacy phones



CleanAir Technical Details





CleanAir Specific Acronyms

- AQI – Air Quality Index – also seen as AQ
- IDR – Interference Device Report
- PMAC – Pseudo MAC
- Merge – Correlation of IDR's based on PMAC
- ZOI – Zone of Impact
- LMAP – Local Mode AP – AP serving clients
- MMAP – Monitor Mode AP – AP scanning all bands

Key Components Interaction

- Information is driven in two ways
 - AQI – Air Quality index reporting
 - IDR – Interference device report
- Air Quality – Is derived by the AP's, Stored on WLC, and polled by WCS
- Interference Device Reports – are reported to WLC
 - WLC will merge multiple IDR's
 - Keep a limited Database (single reporting period)
 - Forward NMSP notification message with IDR payload to MSE

Non Wi-Fi Interference Detection



The CleanAir AP

- Built into the silicon of the Wi-Fi chip is an additional 500K logic gates that house the SAgE logic.
- SAgE is the spectrum analyzer that was used on the Spectrum Expert Cards (Spectrum Analysis Engine)
- Controlling the SAgE hardware is a software known as SensorD – where all measurements are gathered and reported to and from the AP
- SensorD does all classification of devices and calculations required to populate upstream information stores and handles interfacing to CAPWAP

Information passed from the AP to controllers is minimal. No off platform calculations are performed: it all happens on the AP

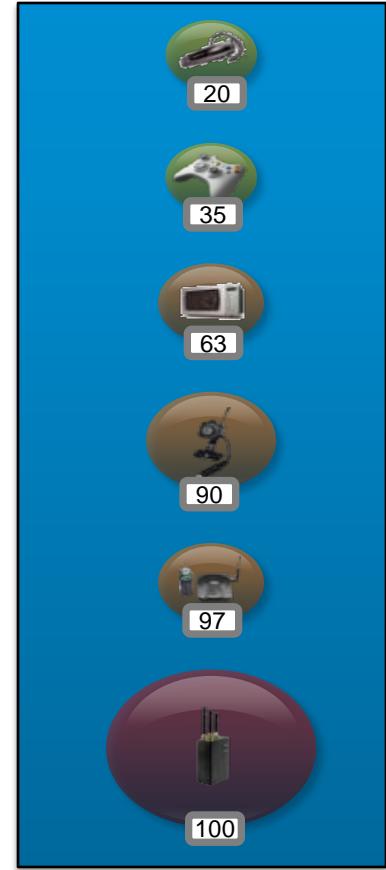
Air Quality Index - AQI

- Air Quality is a measurement of non-wifi and adjacent channel interference
- All Individual devices when Classified are assigned a Severity Value
- Air Quality is a measure of all Devices/Severities within a Radio, Floor, Building, or Campus



Air Quality and Severity

- For each Classified Device – a Severity Value is calculated
- Severity of 0 is not Severe – a Severity of 100 is very severe.
- Severity is a local opinion of the reporting AP and takes into account the type of device, Duty Cycle (persistence) and Power as measured by the AP.
- For the same device – severity will differ on each reporting AP because of the AP's RF relationship to that device.





Supported Interferers

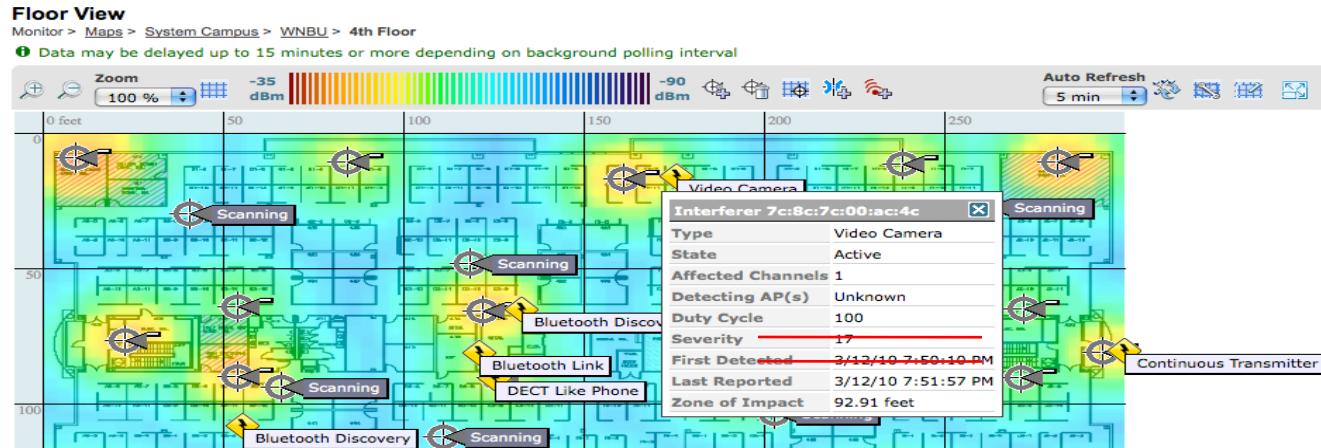
Cisco Unified Wireless Network 7.0 Release

- 2.4 GHz only
 - Bluetooth Link
 - Bluetooth Discovery
 - 802.11FH
 - Microwave Oven
 - Industrial wireless/802.15.4
 - Xbox
- 5 GHz only
 - Radar
 - WiMAX Mobile
 - WiMAX Fixed
- 2.4 or 5 GHz
 - Jammer
 - WiFi Inverted
 - WiFi Invalid Channel
 - Continuous Transmitter
 - Video Camera
 - SuperAG
 - Canopy
 - Other (i.e. unclassified devices)
 - TDD Transmitter
 - DECT-like Phone

1. Classifiers are expandable over time with software upgrade.
2. All third party trademarks are the property of their respective

- **Definite Security Threat Devices**
- **Potential Security Threat Devices**
- **Performance Impacting Devices**

Air Quality and Severity



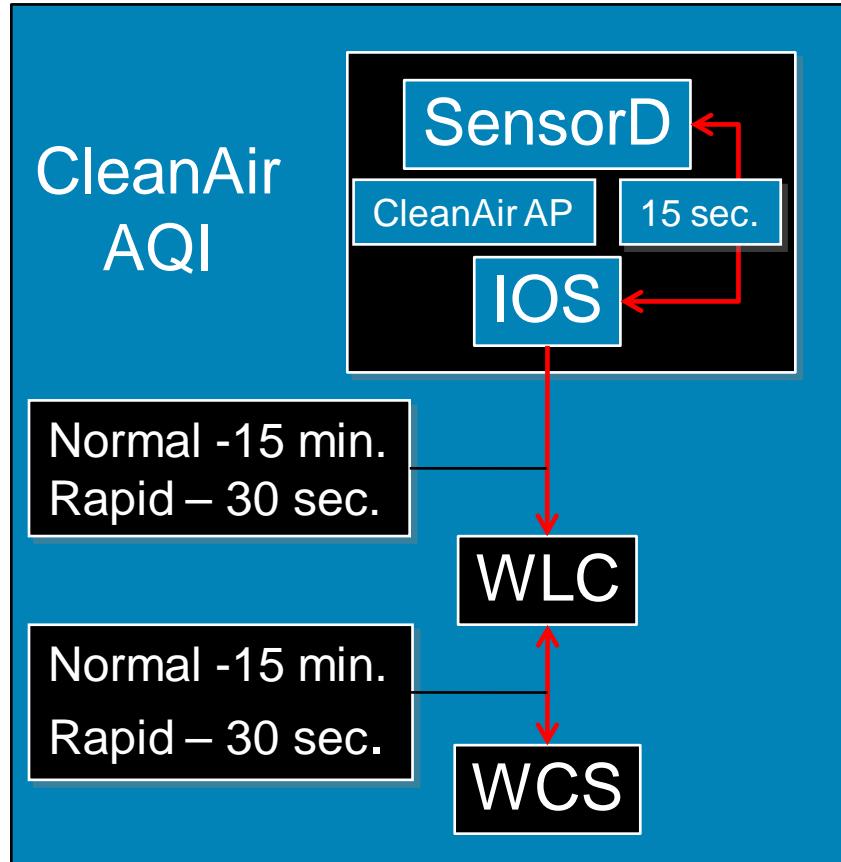
- Severity is used to understand the potential impact to a Wi-Fi network
- The RSSI at the AP for this interferer (-78) is well below CCA threshold (Clear Channel Assessment)
- Even with duty cycle of 100% - the severity here is 17 – if it was closer to us, the severity would be much higher

Air Quality and Severity

- Severity is calculated for a single device
- All devices affecting a radio/channel are added together and subtracted from Air Quality for that for that radio/ served channel
- Separate AQ metrics exist per band
- Air Quality is observable at the Radio/channel level, or averaged together for a Floor, Building, Campus in a hierarchical fashion.

AQ Detail

- AP manages AQI data – averaging period is decided by WCS/WLC, and configured on AP by WLC
- Default AQ Averaging periods are
 - 15 min. default (up to 1 hour)
 - Rapid Update Mode – 30 seconds
- AP-SensorD reports AQ information every 15 seconds to IOS



AQI In-Depth

- Each AQ report contains the average, and the minimum observed AQ during the period
- Each CleanAir Radio sends AQ reports independently to the WLC for the channel it is serving (15 Minutes by default) or all channels if in Monitor Mode (MMAP)
- WLC Maintains last normal AQ report for each radio until update is received
- WCS polls each WLC at predetermined (normal or rapid) intervals (Normal 15 minutes, Rapid 30 second)

AQI Summary

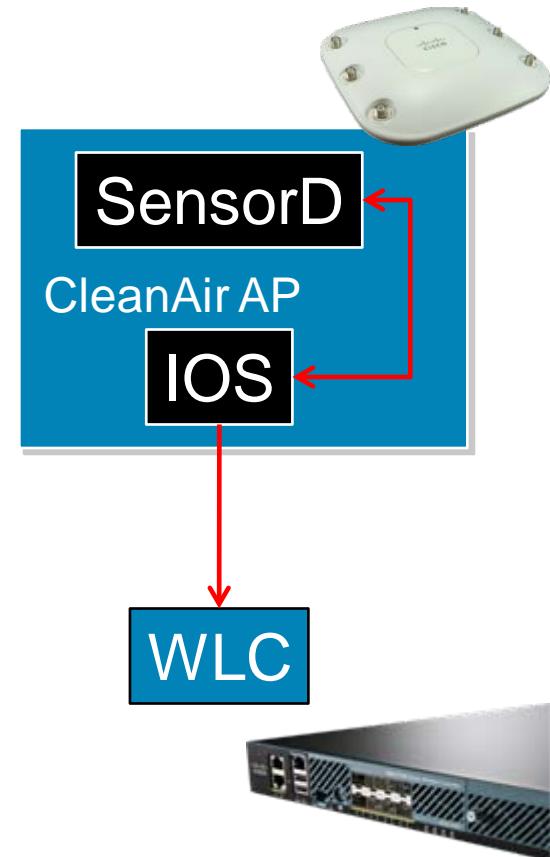
- AQ reports drive the AQI
- AQ is good at 100 and bad at 0
- ED-RRM feature is driven by AQ directly from the AP – independent of the controller or RRM
- Air Quality is a measure of NON Wi-Fi interference and Adjacent Channel Wi-Fi only
- All on channel Wi-Fi is monitored by the Wi-Fi chip, CleanAir is locked out.

Interference Device Report

IDR and The AP

- IDR's are reports of devices classified by SensorD
- Top 10, by severity are reported to WLC
- A Security IDR will always be reported regardless of severity
- IDR up/down reporting is near real time
- AP tracks all IDR's not reported to WLC

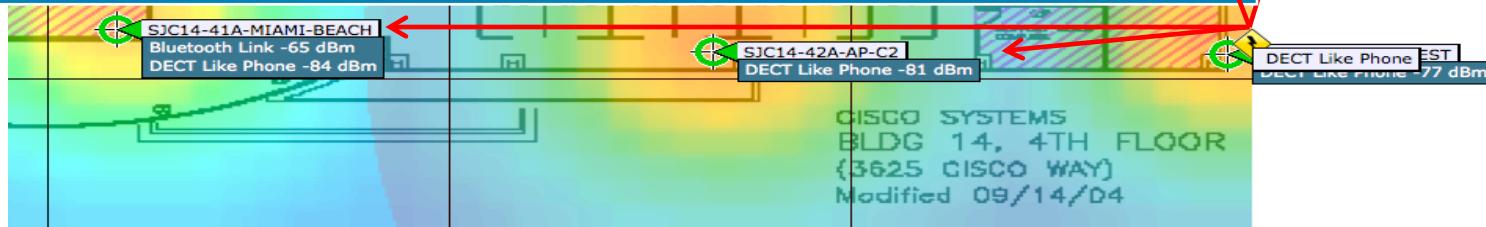
TYPE	SEV	WLC
SEC	1	*
INT	20	*
INT	9	*
INT	2	*
INT	2	*
INT	1	*



Multiple AP's = Multiple Sensors



We see multiple AP tags showing the detection of DECT and the corresponding RSSI. But which ones are really the same device?

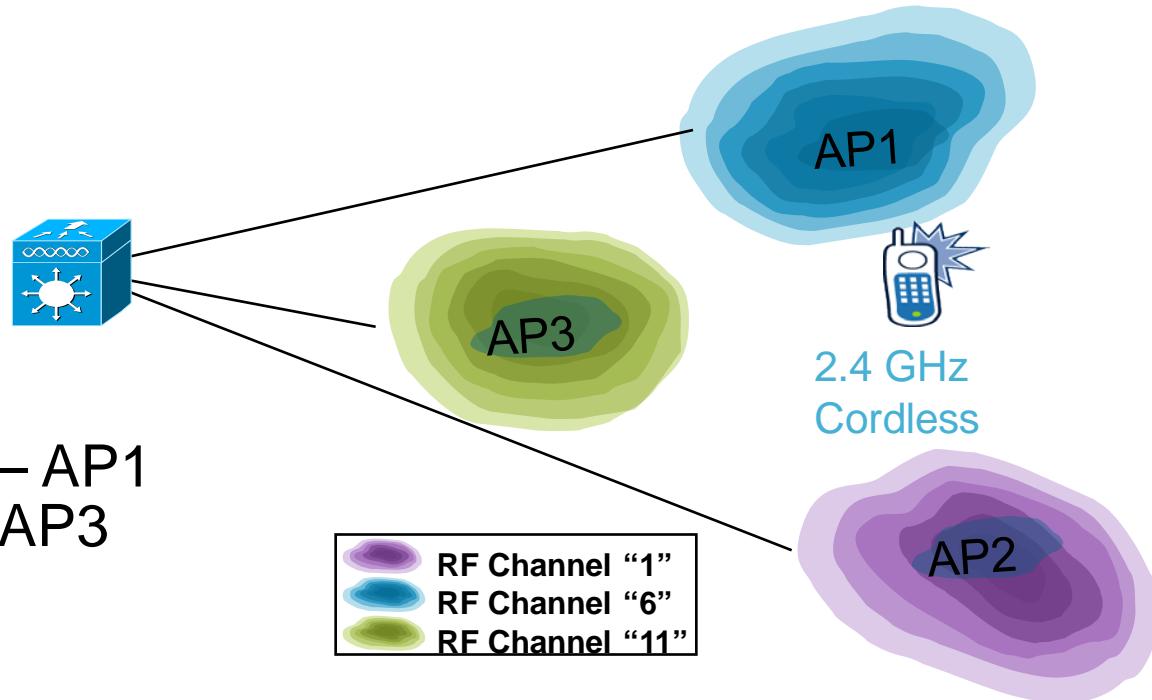


IDR In-Depth – The AP - PMAC

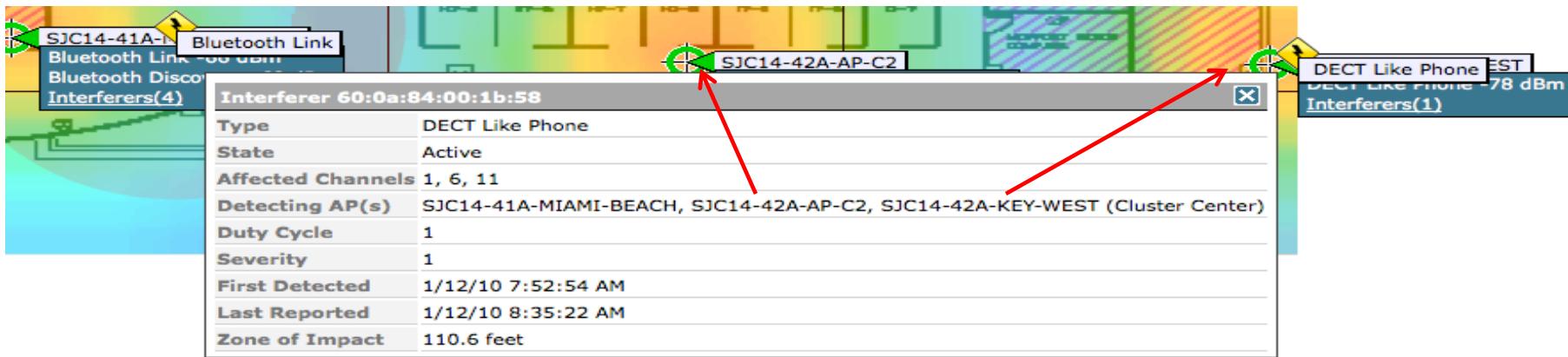
- Pseudo – MAC applied to analog device signatures
- PMAC will never calculate exactly the same on all AP's detecting the same device – but rather similar
- PMAC will change overtime for a given device
 - Battery operated devices – voltage drop – temp variations
 - Measurement accuracy – or inaccuracy
- The AP will combine devices that can not reliably be merged with devices seen by another AP

WLC Merging – and PMAC “The Cluster”

- IDR-DECT – ap1
- IDR-DECT – ap2
- IDR-DECT – ap3
- Merged IDR = DECT – AP1
(cluster center), AP2, AP3



PMAC Merge



- Once the PMAC Signatures are merged – we can identify which AP's are hearing the same device
- Notice the Cluster Center – this is the closest AP to the device

WLC and PMAC Merging

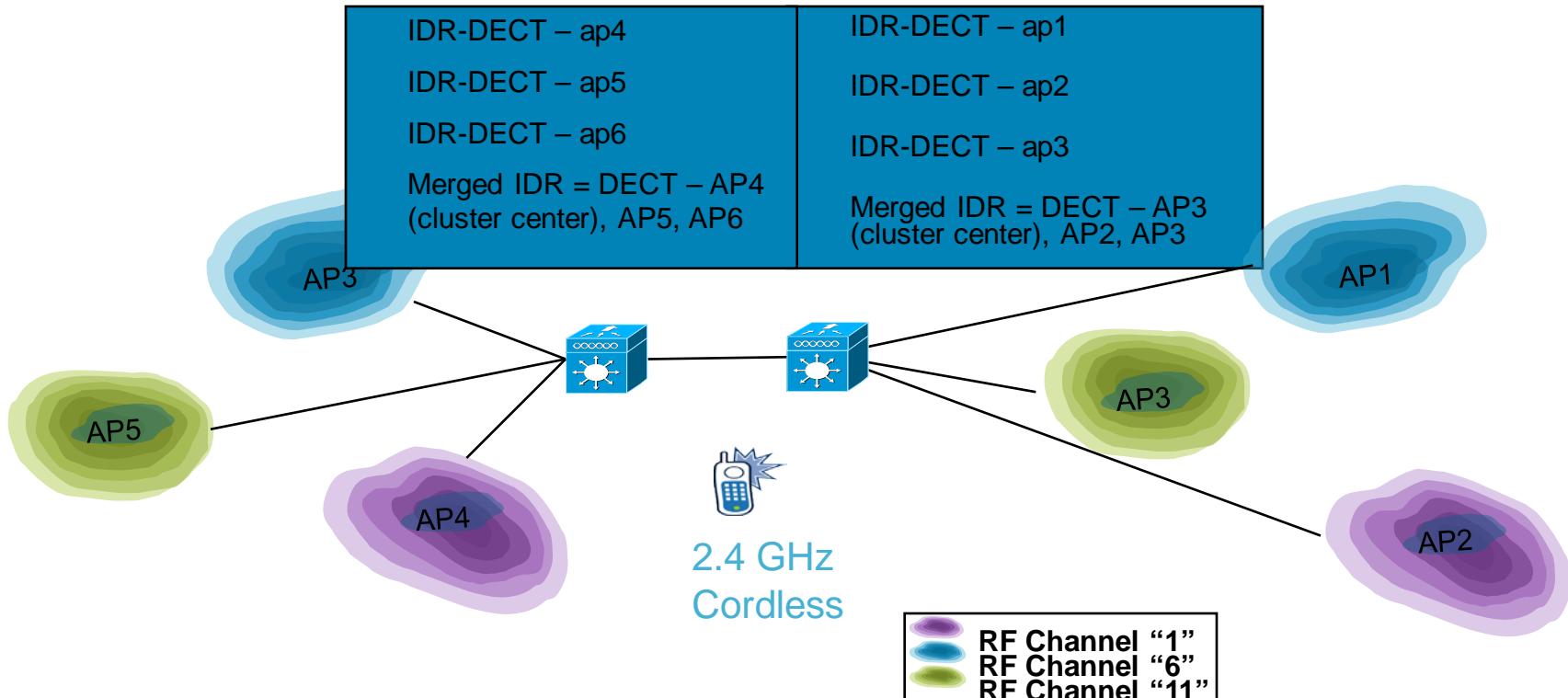
- WLC performs comparison function on received IDR's PMAC
- WLC can merge devices for AP's physically connected to it
- WLC merge results are only viewable in IDR traps sent to trap receiver (WCS)
- No Location is performed on WLC merged interferers
- The result of a WLC merge is forwarded to the MSE (If present) along with all of the supporting IDR's

The MSE

- All IDR's received by a WLC are sent to MSE via NMSP notify with IDR payload
- NMSP message includes the merged IDR and the individual IDR's used for that conclusion
- IDR's are re-merged at the MSE, this accommodates multiple WLC systems
- A tracked Interferer is equal to a client for CAS license purpose – each active merged interferer will consume 1 seat

MSE Merging – LMAP X-WLC

MSE Merge



MSE – WLC Merging and Location

- MSE and the WLC rely 1st on RF Neighbor lists to establish spatial probability in a merge
- LMAP AP's are active and send neighbor messages as part of normal RRM operation
- Changing Neighbor message defaults will affect merging
- MMAP AP's are passive devices and do not send neighbor messages

CleanAir Mitigation Modes



Interference Mitigation Features

- Persistent Device Avoidance – PDA

Operates on Classification – IDR on a per AP basis

Once set – biases DCA against the PDA channel for the detecting AP only

Remembers interference and avoids placing the AP back on the same channel

- Energy Detect – RRM or ED-RRM

Fast acting ($=< 30$ seconds)

Works on AQI on a per AP basis

Designed to prevent catastrophic interference from disrupting channel/clients

NOTE: Only Available with full CleanAir enabled installation – not overlay

PDA - configuration

Save Configuration | Ping | Logout | Refresh

MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

Wireless

Access Points
All APs
Radios
802.11a/n
802.11b/g/n
Global Configuration

Advanced
Mesh
HREAP Groups
802.11a/n
802.11b/g/n
Network
RRM
RF Grouping
TPC
DCA
Coverage
General
Client Roaming
Media
EDCA Parameters
High Throughput
(802.11n)
CleanAir

Media Stream
Country
Timers
QoS

802.11b > RRM > Dynamic Channel Assignment (DCA)

Dynamic Channel Assignment Algorithm

Channel Assignment Method: Automatic (radio button selected), Interval: 10 minutes, AnchorTime: 0, Invoke Channel Update Once

Avoid Foreign AP interference: Enabled (checkbox checked)

Avoid Cisco AP load: Enabled (checkbox checked)

Avoid non-802.11b noise: Enabled (checkbox checked) [highlighted with a red box]

non-WiFi Device Avoidance: Enabled (checkbox checked)

Channel Assignment Leader: 00:24:97:69:9a:60
Last Auto Channel Assignment: 185 secs ago
DCA Channel Sensitivity: Medium (10 dB)

DCA Channel List

DCA Channels: 1, 6, 11

Select Channel: 1, 2, 3, 4, 5, 6

Event Driven RRM

EDRRM: Enabled (checkbox checked)
Sensitivity Threshold: Medium

Enabled Per Band
Same on WCS or WLC
EDRRM has threshold variable

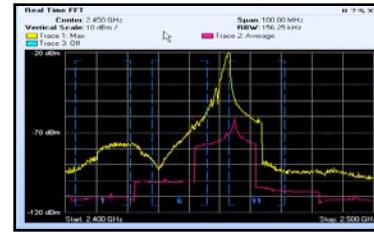
WLC GUI - Wireless=>802.11a/b=>RRM=>DCA

WCS – Configure=>controllers=>802.11a/b=>RRM=>DCA

ED-RRM AQI thresholds:
Low – 35
Medium (default) – 50
High - 60

PDA – Use case

- PDA logs the device for this AP.
- A CM bias is added to this AP's channel 11 only
- The bias works in normal DCA operations to steer the AP away from channel 11 – it does not prevent the AP from re-selecting this channel
- AP remembers this bias for 7 days, which is re-set if the device is seen again within that period
- If DCA determines that the affected AP is best on channel 11 it will be assigned



Microwave Oven detected
Channel 11 – highest
Impact.



PDA Operation

- If channel change is caused by PDA event – it will be logged in WCS – Monitor=>RRM
- PDA event is viewable on WLC=>wireless=>Access Points=>Radios=>802.11a/b=>CleanAir RRM
- Only available with full LMAP deployment
- Microwave Oven, Video Camera, Canopy, Fixed Wi-Fi are all persistent devices

Wireless 802.11b/g/n Radios

Entries 1 - 7 of 7

AP Name	Radio Slot#	Base Radio MAC	Admin Status	Operational Status	Channel	Clean-Air Admin Status	Clean-Air Oper Status	Power Level	Antenna
AP0022.bd18.a642	0	00:22:bd:cc:d4:20	Enable	UP	1	Enable	UP	7	
AP0022.bd18.a916	0	00:22:bd:cc:e5:d0	Enable	UP	6 *	Enable	UP	8	
AP0022.bd18.ab11	0	00:22:bd:cc:de:b0	Enable	UP	11 *	Enable	UP	3	
cisco_1250	0	00:17:df:a6:84:30	Disable	DOWN	1	NA	NA	5	
AP001b.d513.1652	0	00:17:df:a6:e9:70	Disable	DOWN	6 *	NA	NA	8	External
c1130_3	0	00:1a:a2:f1:e2:40	Disable	DOWN	6	NA	NA	8	Internal

802.11b/g/n Cisco APs > AP0022.bd18.ab11 > Persistent Devices

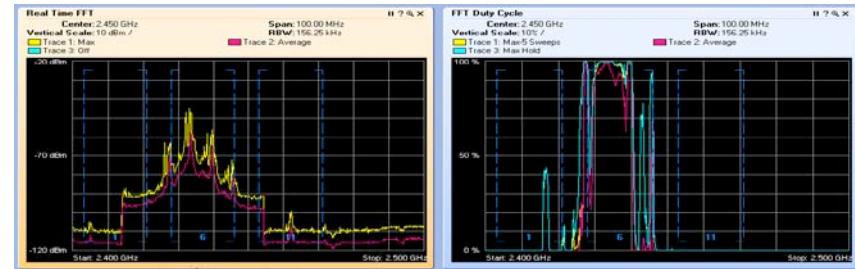
Class Type	Channel	DC(%)	RSSI(dBm)	Last Seen Time
Video Camera	11	100	-64	Tue Mar 16 15:28:10 2010

ED-RRM Operation

- ED-RRM operates based on Air Quality (AQ)
- Each AP measures AQ over a 15 second period and reports it to the controller in as little as 30 second increments (rapid update mode)
- ED-RRM is designed to instantly sense a catastrophic interference source defined as a high duty cycle interferer – and if the AQI drops perilously – immediately change the AP's channel independent of RRM.
- ED-RRM prevents the AP from returning to the original channel for 3 hours after the event.
- Channel Change reason is logged in Monitor RRM as catastrophic AQI event

ED-RRM Use Case

Video camera produces 100% DC
If seen at an AP above CCA threshold
the AP will stop beaconing, clients
will not attempt to associate



- The AP reacts almost instantly (within 30 seconds)
- Clients that have decent roaming capabilities will reconnect
- ED-RRM AQI thresholds are:

Low – 35

Medium (default) – 50

High - 60

Spectrum Monitoring



WCS - Home



- WCS version 7.0.x includes the CleanAir information Tab
- The Alarm Summary Panel will display both AQ alerts under Performance and Security Alerts under Security
- Advanced Search function includes Interference – rich interface for searches

WCS – CleanAir TAB

The image shows the Cisco WCS CleanAir TAB interface. On the left, there are four line graphs showing Average Air Quality (AQ) over time for 802.11a/n and 802.11b/g/n, both average and minimum. On the right, there are four corresponding boxes with labels: "802.11a average AQ", "802.11b average AQ", "802.11a Minimum AQ", and "802.11b Minimum AQ". To the right of these graphs is a red-bordered box containing text and two smaller graphs. The text reads: "Requires MSE to display Worst 802.11a/b interferers". It points to a section titled "Worst 802.11a/b Interferers" which contains error messages and a graph of "Interferer Count" over time. Below this is another graph for "802.11b/g/n Interferer Count". At the bottom right is a table titled "Recent Security-risk Interferers" with several entries. A large blue box at the bottom right is labeled "Recent Security IDR's".

Requires MSE to display
Worst 802.11a/b interferers

802.11a average AQ

802.11b average AQ

802.11a Minimum AQ

802.11b Minimum AQ

Worst 802.11a/b Interferers

Error loading 'DashboardComponentAction.do?command=load&componentId=3866' (0)

Worst 802.11b/g/n Interferers

Error loading 'DashboardComponentAction.do?command=load&componentId=3867' (0)

802.11a/n Interferer Count

6h 1d 1w 2w 4w 3m 6m 1y Cu

Interferer Count

1

0

802.11b/g/n Interferer Count

6h 1d 1w 2w 4w 3m 6m 1y Cu

Interferer Count

4

3

2

1

0

Recent Security-risk Interferers

Type	Severity	Affected Channels	Last Updated	Detecting AP
DECT Like Phone	1	1	3/16/10 4:04 PM	AP0022_bd18_a642
DECT Like Phone	2	1, 6, 11	3/16/10 3:44 PM	AP0022_hd18_d496
DECT Like Phone	3	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11	3/16/10 3:42 PM	AP0022_bd18_a611
DECT Like Phone	1	1	3/12/10 2:45 AM	AP0022_bd18_a642
DECT Like Phone	3	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11	3/11/10 3:12 PM	AP0022_bd18_87c0
WiFi Invalid Channel				18.87c0
DECT Like Phone				18_a642
DECT Like Phone				18_a642
DECT Like Phone				18.87c0
DECT Like Phone				18.87c0

Recent Security IDR's

WCS – Alarm Summary

The screenshot shows two views of the Cisco WCS Alarm Summary interface. The left view is a summary table with categories like Access Points, Controllers, and Malicious AP, each with a red triangle icon indicating 25 alarms. The right view is a detailed list of alarms under the 'Alarms' tab, showing columns for Severity, Failure Source, Owner, Date/Time, and Message. The messages describe Air Quality Index threshold violations across various wireless interfaces.

Severity	Failure Source	Owner	Date/Time*	Message	Acknowledged
Info	AP AP0022_0d18.ap11, Interface 802.11b/g/n		1/19/10 8:36:19 AM	Air Quality Index on Channel '9' is '92' (Threshold:'85').	No
Info	AP AP0022_0d18.ap42, Interface 802.11b/g/n		1/19/10 8:35:22 AM	Air Quality Index on Channel '1' is '46' (Threshold:'85').	No
Info	AP AP0022_0d18.ap96, Interface 802.11b/g/n		1/19/10 8:24:26 AM	Air Quality Index on Channel '1' is '35' (Threshold:'85').	No
Info	AP AP0022_0d18.ap11, Interface 802.11b/g/n		1/19/10 8:49:35 AM	Air Quality Index on Channel '1' is '2' (Threshold:'85').	No
Info	AP AP0022_0d18.87c0, Interface 802.11b/g/n		1/18/10 3:51:19 PM	Air Quality Index on Channel '6' is '79' (Threshold:'85').	No
Info	AP AP0022_0d18.87c0, Interface 802.11b/g/n		1/18/10 2:20:02 PM	Air Quality Index on Channel '1' is '33' (Threshold:'85').	No
Info	AP AP0022_0d18.87c0, Interface 802.11b/g/n		1/17/10 8:01:45 PM	Air Quality Index on Channel '11' is '95' (Threshold:'85').	No
Info	AP AP0022_0d18.87c0, Interface 802.11a/n		1/17/10 2:16:56 AM	Air Quality Index on Channel '157' is '98' (Threshold:'85').	No

- Performance alarms report AQ threshold violations
- Security Alarms Report security IDR instances
- CleanAir Alarms and Traps configured from Configure=>Controllers=>802.11a/b=>CleanAir

CleanAir

SNMP Trap Settings/controls

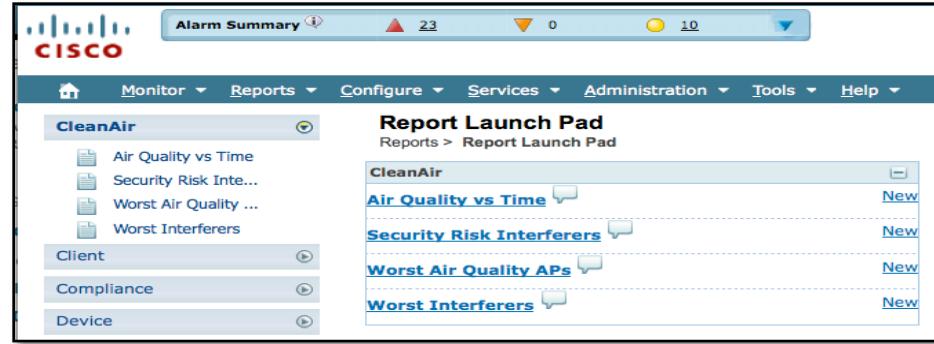
- Select trap configurations per band
- Select which interference
- Enable/Disable AQ threshold alert
- Select Interference types for Security alert trap

The screenshot shows the Cisco Wireless Controller interface under the 'WIRELESS' tab. On the left, a navigation tree includes 'Access Points', 'Advanced', 'Mesh', 'HREAP Groups', '802.11a/n', '802.11b/g/n', 'RRM', 'Coverage', 'General', 'Client Roaming', 'Media', 'EDCA Parameters', 'High Throughput', 'CleanAir', 'Media Stream', 'Country', 'Timers', and 'QoS'. The 'CleanAir' node is expanded. The main pane displays '802.11b > CleanAir' settings. It has sections for 'CleanAir Parameters' (with 'CleanAir' and 'Report Interferers' checkboxes), 'Interferences to Detect' (listing 'Bluetooth Sco Acl', 'Microwave', 'Spectrum 802 11 FH', 'Bluetooth Paging Inquiry', and 'Generic TDD'), 'Trap Configurations' (with 'Enable AQI(Air Quality Index) Trap' and 'AQI Alarm Threshold (1 to 100)' set to 85), 'Trap on these types' (listing 'Jammer', 'Spectrum 802.11 inverted', and 'Spectrum 802.11 non std channel'), and 'Do not trap on these types' (listing 'Bluetooth Sco Acl', 'Microwave', 'Spectrum 802 11 FH', 'Bluetooth Paging Inquiry', and 'Generic TDD'). A note at the bottom states: '(1)Device Security alarms, Event Driven RRM and Persistence Device Avoidance algorithm will not work if Interferers reporting is disabled. (2)AQI value 100 is best and 1 is worst.'

Granular control over trap messages for performance thresholds as well as security concerns

WCS CleanAir reports

- CleanAir reports allow configuration by floor-controller-AP and radio
- Air Quality and Security Risk Reports are all functional without MSE
- Worst Interference report requires MSE



WCS CleanAir Maps

The screenshot shows the Cisco WCS interface with the following details:

- Header:** Alarm Summary (22), Wireless Control System, User: root, Advanced Search, Logout.
- Left Sidebar:** CISCO logo, Monitor, Reports, Configure, Services, Administration, Tools, Help, Maps Tree View, Maps (Root Area), System Campus.
- Middle Panel:** Maps (Edit View) table showing air quality data for different locations. The table has columns: Name, Type, Total APs, a/n Radios, b/g/n Radios, Critical Radio Alarms, Clients, Status, a/n Avg Air Quality, a/n Min Air Quality, b/g/n Avg Air Quality, and b/g/n Min Air Quality.

Name	Type	Total APs	a/n Radios	b/g/n Radios	Critical Radio Alarms	Clients	Status	a/n Avg Air Quality	a/n Min Air Quality	b/g/n Avg Air Quality	b/g/n Min Air Quality
System Campus	Campus	5	5	5	0	3	Yellow	99	98	97	97
System Campus > Home	Building	5	5	5	0	2	Yellow	99	98	97	97
System Campus > Home > 1st	Floor Area	0	0	0	0	0	Green	Not Available	Not Available	Not Available	Not Available
System Campus > Home > 2nd	Floor Area	0	0	0	0	0	Green	Not Available	Not Available	Not Available	Not Available
System Campus > Home > basement	Floor Area	5	5	5	0	3	Yellow	99	98	97	97

- Bottom Panel:** A summary table showing average and minimum air quality values for each location type. The table has columns: a/n Avg Air Quality, a/n Min Air Quality, b/g/n Avg Air Quality, and b/g/n Min Air Quality.

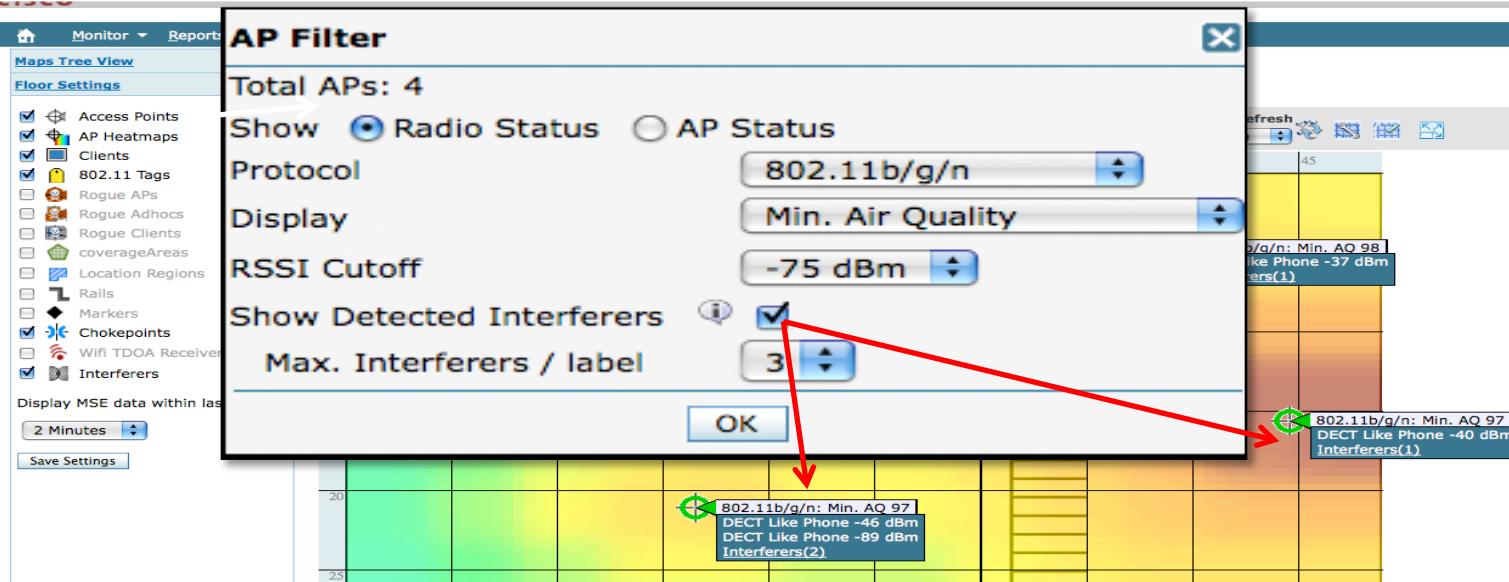
a/n Avg Air Quality	a/n Min Air Quality	b/g/n Avg Air Quality	b/g/n Min Air Quality
99	98	97	97
99	98	97	97
Not Available	Not Available	Not Available	Not Available
Not Available	Not Available	Not Available	Not Available
99	98	97	97

CleanAir Air Quality reports per radio and is averaged up:
By AP, By Floor, By Building, and by Campus

Select Edit View to add CleanAir Average and Minimum readings to the Maps View

WCS CleanAir Maps

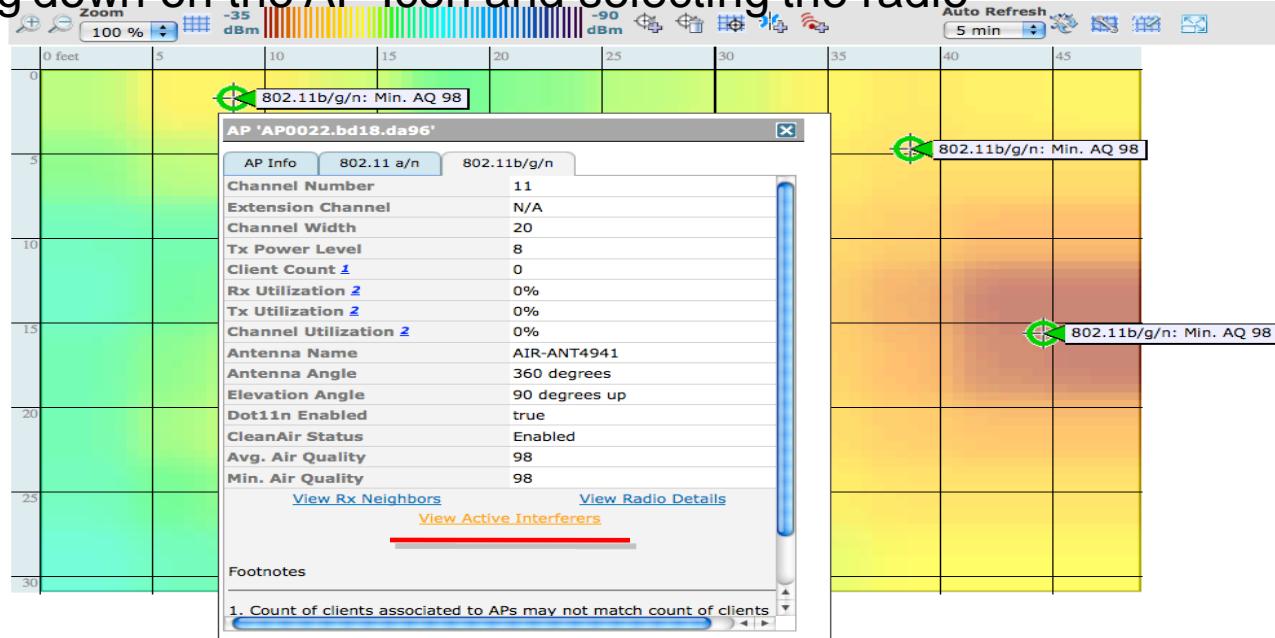
Selecting a map for a given floor provides detail relevant to the selected floor. You can change the AP tags to display CleanAir information such as CleanAir Status (shows which AP's are capable), Min or average AQ values, or Average and Minimum values. The values are relevant to the band selected.



Interferers displayed in this way do not require MSE – However they are Raw and not coordinated to eliminate duplicates

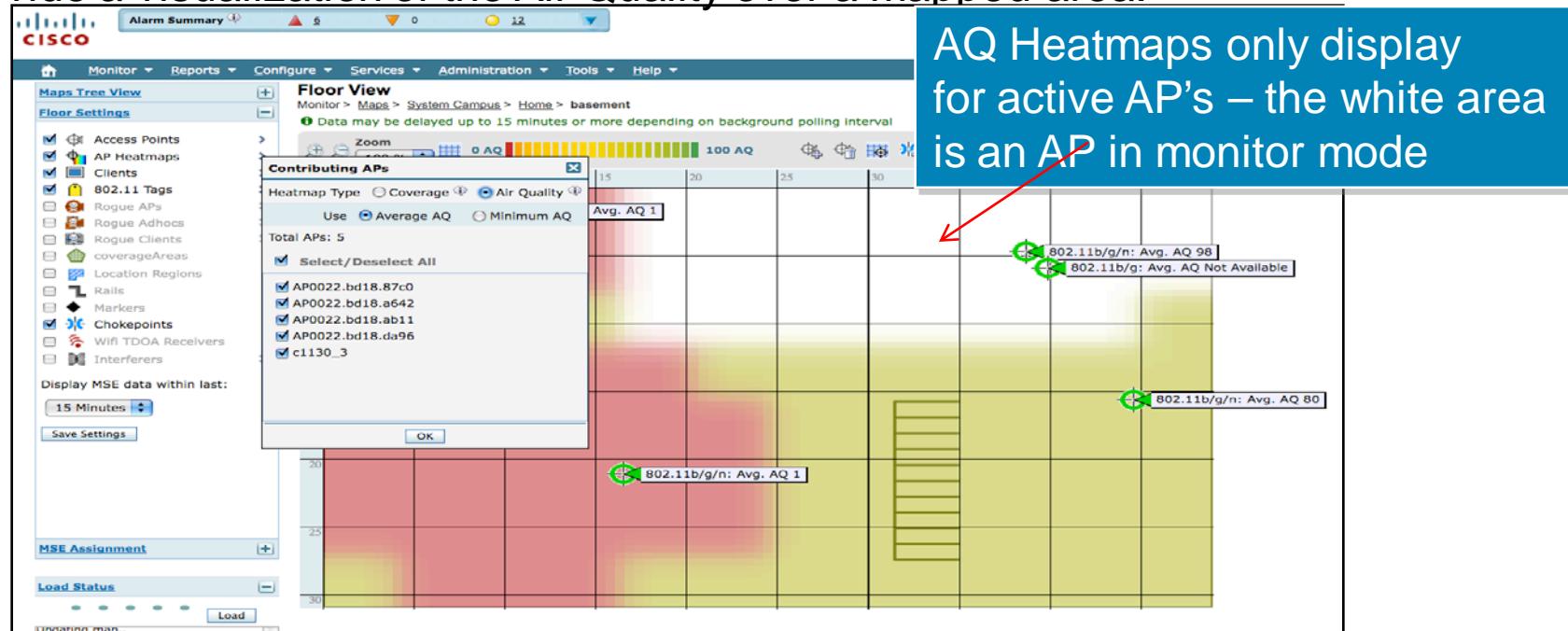
WCS CleanAir Maps

You can also view interference information being seen on any radio interface by drilling down on the AP Icon and selecting the radio



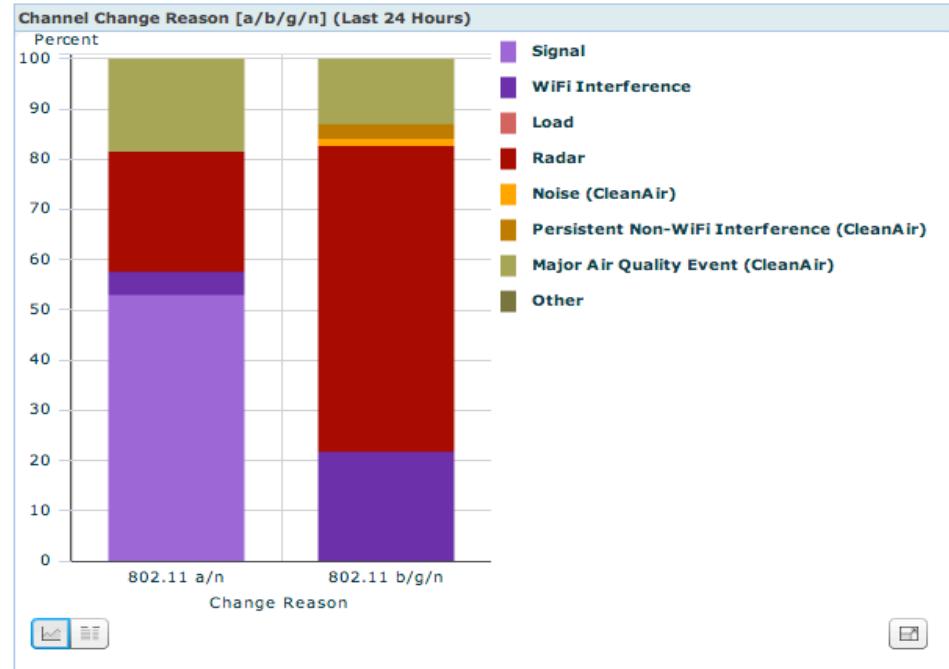
WCS CleanAir Maps

Air Quality heatmaps can be selected to represent average or minimum AQ and Provide a visualization of the Air Quality over a mapped area.



WCS – RRM Dashboard

- RRM Dashboard has been modified to capture CleanAir metrics
- Persistent device (PDA)
- Major Air Quality (ED-RRM)
- Noise



WCS CleanAir enabled Security Dashboard

CleanAir designated Security devices are integrated with the Security dashboard

The screenshot shows the Cisco WCS Home interface with the 'Security' tab selected. The main area displays various security metrics and event logs. A red arrow points to the 'Adhoc Requests' link under the 'CleanAir Security' section.

Security Index:
Score: 60.84%
Top Security Issues: MFP Client Protection, WLAN Interface, Weak encryption method, SNMP v1/v2, Mobility Services Engine user has default password configured.

Malicious Rogue APs:
Last Hour: 0, Last 24 Hours: 0, Total Active: 0
None detected.

Unclassified Rogue APs:
Last Hour: 0, Last 24 Hours: 0, Total Active: 0
Alert: 0, 0, 0.

Friendly Rogue APs:
Last Hour: 0, Last 24 Hours: 0, Total Active: 0
Internal: 0, External: 0.

CleanAir Security:
CleanAir Security
Last Hour: 0, 24 Hours: 0, Total Active: 0
Security-risk Devices
Last Hour: 0, 24 Hours: 1, Total Active: 1

Attacks Detected:
wIPS Denial of Service Attacks: Last Hour: 0, 24 Hours: 0, Total Active: 0
wIPS Security Penetration Attacks: Last Hour: 0, 24 Hours: 0, Total Active: 0
Custom Signature Events: Last Hour: 0, 24 Hours: 0, Total Active: 0
None detected.

Cisco Wired IPS Events:
Cisco Wired IPS Events: Last Hour: 0, 24 Hours: 0, Total Active: 0
None detected.

AP Threats/Attacks:
AP Threats/Attacks: Last Hour: 0, 24 Hours: 0, Total Active: 0
None detected.

HIP-Attacks:
MFP Attacks: Last Hour: 0, 24 Hours: 0, Total Active: 0
None detected.

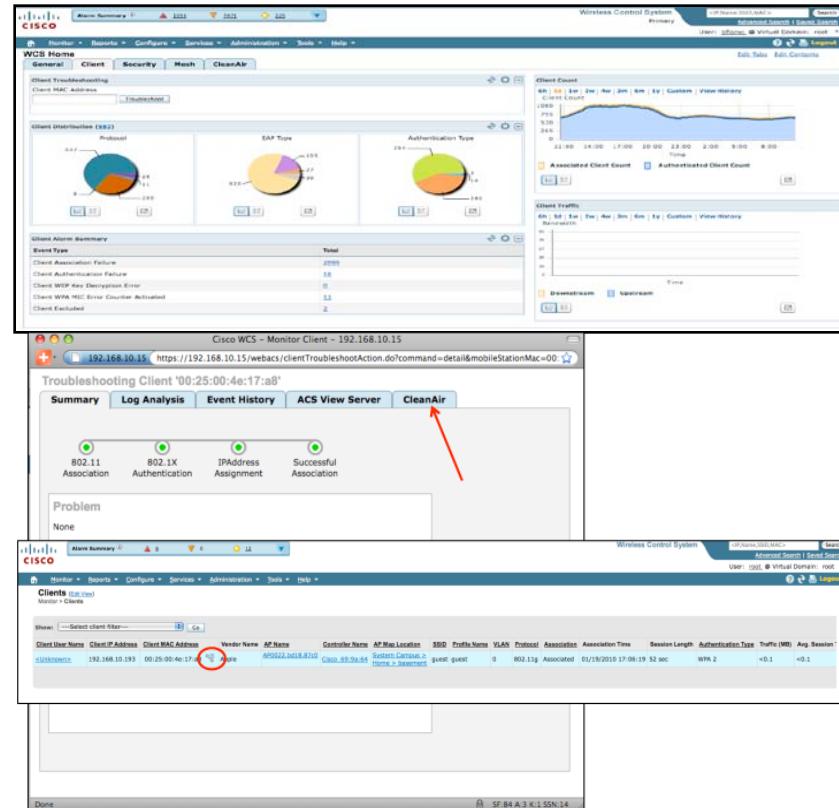
Client Security Events:
Client Security Events: Last Hour: 0, 24 Hours: 0, Total Active: 0

WCS CleanAir Security

- There are three devices enabled by Default for security – And not a single WIDs/WIPs solution on the market can see them
- The customer can also add any other device that they deem appropriate
 - Jammer
 - Wi-Fi Inverted
 - Wi-Fi Invalid channel
- Jammers – are self explanatory – and readily available online
- Wi-Fi inverted is simply inverting the I and the Q of the RF signal – very effective
- Off Channel is a fairly easy hack with DD-WRT – simply moving the center frequency by a few KHz will render it invisible.

WCS CleanAir Client Troubleshooting integration

- CleanAir information is also coordinated into the client troubleshooting dashboard
- Selecting a client – and launching the client TS dashboard now adds a CleanAir tab
- The TAB displays any interference source that is currently being detected by the AP the client is attached to



WCS CleanAir Client TS integration

Cisco WCS – Monitor Client – 192.168.10.15
192.168.10.15 https://192.168.10.15/webacs/clientTroubleshootAction.do?command=detail&mobileStationMac=00:25:00:4e:17:a8

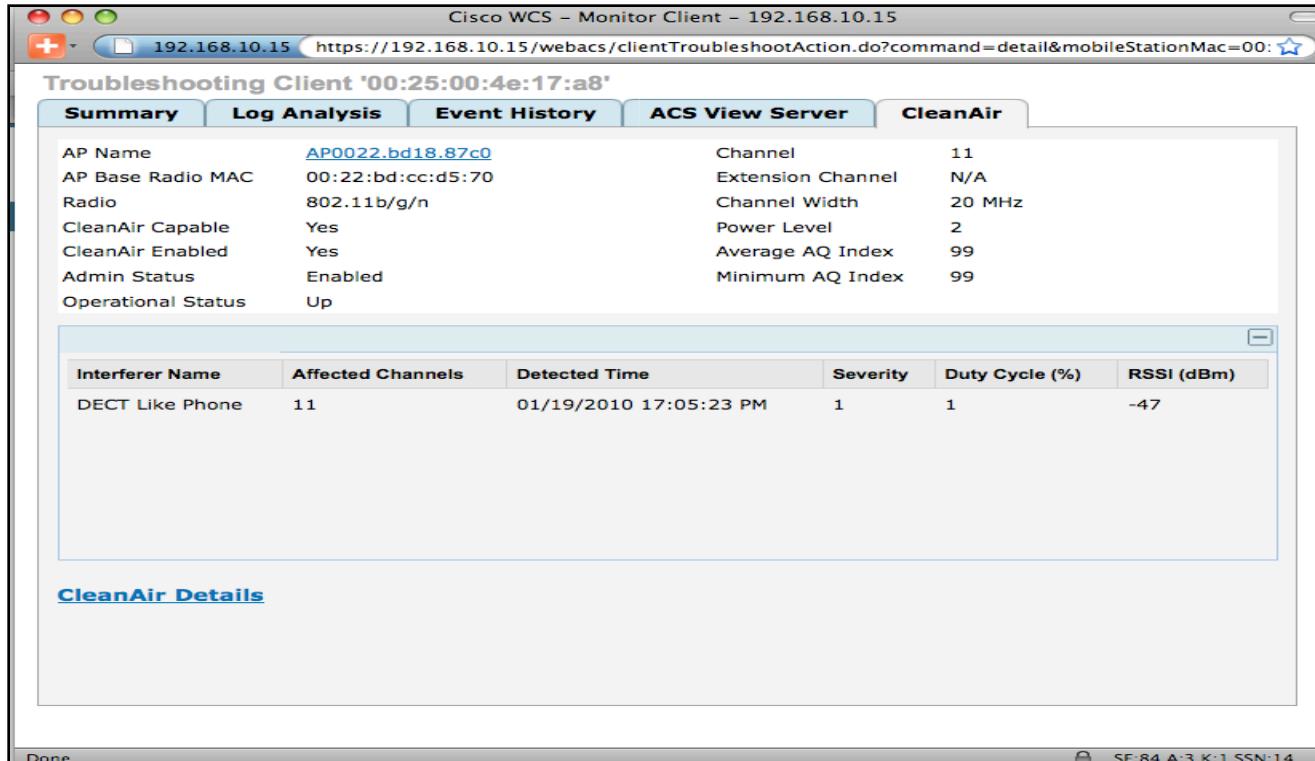
Troubleshooting Client '00:25:00:4e:17:a8'

Summary	Log Analysis	Event History	ACS View Server	CleanAir
AP Name AP Base Radio MAC Radio CleanAir Capable CleanAir Enabled Admin Status Operational Status	AP0022.bd18.87c0 00:22:bd:cc:d5:70 802.11b/g/n Yes Yes Enabled Up	Channel Extension Channel Channel Width Power Level Average AQ Index Minimum AQ Index	11 N/A 20 MHz 2 99 99	

Interferer Name	Affected Channels	Detected Time	Severity	Duty Cycle (%)	RSSI (dBm)
DECT Like Phone	11	01/19/2010 17:05:23 PM	1	1	-47

[CleanAir Details](#)

Done SF:84 A:3 K:1 SSN:14



CleanAir Configuration



CleanAir WLC enable (WCS identical under Configure=>Controllers)

The screenshot shows the Cisco Wireless Controller (WLC) interface under the 'Wireless' tab. The '802.11b > CleanAir' section is highlighted. On the right, a blue box contains the text: 'Wireless=>802.11a/b=>CleanAir'. Below this, another blue box contains the following text:

CleanAir is enabled by Default on the AP Interface
it is disabled Globally by default on the controller.

On the left sidebar, 'CleanAir' is listed under '802.11b/g/n' > 'Network' > 'RRM'. In the main pane, the 'CleanAir Parameters' section shows two checkboxes labeled 'Enabled' which are checked and highlighted with a red box. The 'Interferences to Detect' list includes: Bluetooth Sco Acl, Microwave, Spectrum 802.11 FH, Bluetooth Paging Inquiry, Generic TDD. The 'Trap Configurations' section shows 'Enable AQI(Air Quality Index) Trap' and 'AQI Alarm Threshold (1 to 100)' set to 85, both checked and highlighted with a red box. The 'Trap on these types' list includes: Jammer, Spectrum 802.11 inverted, Spectrum 802.11 non std channel. The 'Do not trap on these types' list includes: Bluetooth Sco Acl, Microwave, Spectrum 802.11 FH, Bluetooth Paging Inquiry, Generic TDD. At the bottom, a box contains the command: 'WLC CLI (Cisco Controller) >config 802.11a/b cleanair enable'. A small note at the bottom says '(2)AQI value 100 is best and 1 is worst'.

Per AP radio CleanAir Feature Enable

- Enabled by default – but the first place to check -

The screenshot shows the Cisco Wireless configuration interface for 802.11a/n Cisco APs. The 'CleanAir' section is highlighted with a red box.

General

- AP Name: AP0022.bd18.ab11
- Admin Status: Enable
- Operational Status: UP
- Slot #: 1

11n Parameters

- 11n Supported: Yes
- ClientLink:

CleanAir

- CleanAir Capable: Yes
- CleanAir Status: Enable
- Number of Spectrum Expert connections: 0

RF Channel Assignment

- Current Channel: 153 (Extension : 149)
- Channel Width: 40 MHz
- * Channel width can be configured only when channel configuration is in custom mode
- Assignment Method:
 - Global
 - Custom 153

Tx Power Level Assignment

- Current Tx Power Level: 1
- Assignment Method:
 - Global
 - Custom

Performance Profile

Note: Changing any of the parameters causes the Radio to be temporarily disabled and thus may result in loss of connectivity for some clients.

WCS CleanAir Status

The screenshot shows the Cisco WCS Access Points page. A red box highlights the 'Access Points' link in the top navigation bar. Another red box highlights the 'CleanAir Capable' column in the main table, which lists various access points with their respective CleanAir Capable status (Yes or No). The table also includes columns for AP Name, Ethernet MAC, IP Address, Radio, Map Location, Controller, Client Count, Admin Status, AP Mode, Oper Status, Alarm Status, Channel Number, CleanAir Sensor Status, and CleanAir Status.

AP Name	Ethernet MAC	IP Address	Radio	Map Location	Controller	Client Count	Admin Status	AP Mode	Oper Status	Alarm Status	CleanAir Capable	Channel Number	CleanAir Sensor Status	CleanAir Status
AP022_bd18_87c0	00:22:bd:18:87:c0	192.168.10.89	802.11b/g/n	System Campus > Home > basement	192.168.10.8	1	Enabled	Local	Up	Green	Yes	11	Up	Enabled
AP022_bd18_87c0	00:22:bd:18:87:c0	192.168.10.89	802.11a/n	System Campus > Home > basement	192.168.10.8	1	Enabled	Local	Up	Green	Yes	64	Up	Enabled
AP022_bd18_ab11	00:22:bd:18:ab:11	192.168.10.88	802.11b/g/n	System Campus > Home > basement	192.168.10.8	0	Enabled	Local	Up	Green	Yes	11	Up	Enabled
AP022_bd18_ab11	00:22:bd:18:ab:11	192.168.10.88	802.11a/n	System Campus > Home > basement	192.168.10.8	0	Enabled	Local	Up	Green	Yes	153	Up	Enabled
AP022_bd18_ab42	00:22:bd:18:a6:42	192.168.10.67	802.11b/g/n	System Campus > Home > basement	192.168.10.8	0	Enabled	Local	Up	Green	Yes	1	Up	Enabled
AP022_bd18_ab42	00:22:bd:18:a6:42	192.168.10.67	802.11a/n	System Campus > Home > basement	192.168.10.8	0	Enabled	Local	Up	Green	Yes	48	Up	Enabled
c1130_3	00:1b:0c:92:b1:2c	192.168.10.68	802.11b/g	System Campus > Home > basement	192.168.10.8	0	Disabled	Local	Down	Red	No	6	N/A	N/A
c1130_3	00:1b:0c:92:b1:2c	192.168.10.68	802.11a	System Campus > Home > basement	192.168.10.8	0	Disabled	Local	Down	Red	No	64	N/A	N/A
AP001b_d513_1652	00:1b:d5:13:16:52	192.168.10.79	802.11b/g/n	Unassigned	192.168.10.8	0	Disabled	Local	Down	Red	No	6	N/A	N/A
AP001b_d513_1652	00:1b:d5:13:16:52	192.168.10.79	802.11a/n	Unassigned	192.168.10.8	0	Disabled	Local	Down	Red	No	153	N/A	N/A
AP022_bd18_da96	00:22:bd:18:da:96	192.168.10.50	802.11b/g/n	System Campus > Home > basement	192.168.10.8	0	Enabled	Local	Up	Green	Yes	6	Up	Enabled
AP022_bd18_da96	00:22:bd:18:da:96	192.168.10.50	802.11a/n	System Campus > Home > basement	192.168.10.8	0	Enabled	Local	Up	Green	Yes	36	Up	Enabled
cisco_1250	00:1b:d5:13:1a:96	192.168.10.97	802.11b/g/n	Unassigned	192.168.10.8	0	Disabled	Local	Down	Red	No	1	N/A	N/A
cisco_1250	00:1b:d5:13:1a:96	192.168.10.97	802.11a/n	Unassigned	192.168.10.8	0	Disabled	Local	Down	Red	No	64	N/A	N/A

- Monitor=>Access Points
- Edit View – add CleanAir Status and CleanAir Capable
- CleanAir sensor status –

MSE – Context Aware

WCS=>Services=>MSE=>Context Aware Service=>Administration=>tracking parameters

The screenshot shows the 'Tracking Parameters' configuration for the 'mse' service. The 'Interferers' tracking parameter is highlighted with a red box and a callout box stating 'Disabled by Default'. The 'Active Value' for Interferers is set to 2.

Enable	Tracking Parameters	Enable Limiting	Limit Value	Active Value
<input checked="" type="checkbox"/>	Wired Clients	<input type="checkbox"/>	0	0
<input checked="" type="checkbox"/>	Wireless Clients	<input type="checkbox"/>	0	10
<input type="checkbox"/>	Rogue Clients and AccessPoints	<input type="checkbox"/>	0	0
<input type="checkbox"/>	Exclude Advertised Rogue APs	<input type="checkbox"/>	0	0
<input checked="" type="checkbox"/>	Interferers	<input type="checkbox"/>	0	2

SNMP Parameters

SNMP Retry Count	3	0 - 99999
SNMP Timeout	5	0 - 99999 secs

SNMP Polling Interval

Client Stations	300	1 - 99999 secs
Active RFID Tags	600	1 - 99999 secs
Rogue Clients and AccessPoints	600	1 - 99999 secs
Statistics	900	1 - 99999 secs

Save Cancel

MSE – Context Aware - History

WCS=>Services=>MSE=>Context Aware Service=>Administration=>History Parameters

The screenshot shows the Cisco Wireless Control System (WCS) interface. The top navigation bar includes 'Alarm Summary' with counts for critical (9), minor (0), and warning (15) events, and search fields for IP, Name, SSID, MAC, and a user dropdown for 'root'. The main menu has links for Monitor, Reports, Configure, Services, Administration, Tools, and Help. Under 'Services', 'Mobility Services' is selected, followed by 'mse', 'Context Aware Service', and finally 'Administration > History Parameters'. The left sidebar under 'Context Aware Service' shows various parameters like General, Administration, Tracking Parameters, Filtering Parameters, History Parameters (which is selected and highlighted in blue), Presence Parameters, Import Asset, Information, Export Asset, Wired, Advanced, Partner Engine, and Notification Statistics. The 'History Parameters' page displays settings for archiving data for 30 days, pruning data starting at 23 hours and 50 minutes, and enabling history logging for location transitions. It also lists options for Client Stations, Wired Stations, Asset Tags, Rogue Clients and Access Points, and Interferers. A red box highlights the 'Enable History Logging of Location Transitions for' section, and another red box highlights the 'Interferers' checkbox. A callout box with a black border and white text states 'Disabled by Default' with an arrow pointing to the 'Interferers' checkbox.

- Cisco CleanAir design Guide
 - http://www.cisco.com/en/US/products/ps10315/products_tech_note09186a080b4bdc1.shtml
- Cisco CleanAir – White Papers
 - http://www.cisco.com/en/US/netsol/ns1070/networking_solutions_white_papers_list.html
- CleanAir TechWise TV Broadcast
 - http://www.cisco.com/en/US/solutions/ns340/ns339/ns638/ns914/html_TWT_V/twtv_episode_67.html
- Cisco AP3500 – CleanAir
 - <http://www.cisco.com/en/US/products/ps10981/index.html>

