Solution Guide

WiFi Spectrum Analysis

SEPTEMBER 2014

This document discusses the typical RF interference considerations and challenges of operating a WiFi network in modern enterprise environments, and outlines how the Cisco Meraki Auto RF algorithms and spectrum analysis tools can assist in deploying and maintaining a high-performance WiFi network.

Table of Contents

Introduction

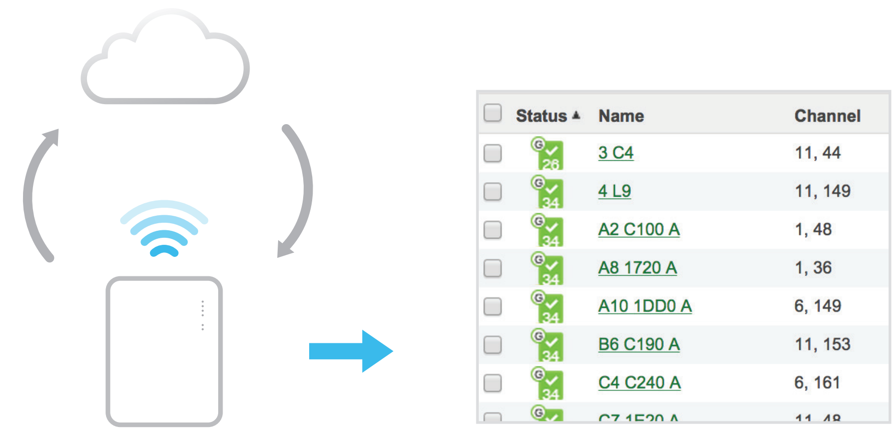
Robust, high-performance wireless access has quickly become a baseline expectation in modern enterprise environments. Due to the widespread consumerization of WiFi devices, interference is increasingly prevalent; as the number of wireless devices increases, so does the amount of interference. In addition, WiFi can suffer from performance degradation due to other sources, including co-channel interference from adjacent WiFi access points (APs), and interference from non-WiFi sources such as Bluetooth devices and security cameras.

Given the emerging enterprise WiFi requirements and challenges, it is recommended that modern WiFi equipment come equipped with complete tools for automatic interference detection and mitigation. The feature set provided by an enterprise WiFi vendor should be two-fold:

- automated RF channel interference detection and mitigation logic; and
- power tools for admins wishing to troubleshoot at deeper layers of the RF environment and manually adjust radio settings.

The Cisco Meraki cloud-managed wireless solution portfolio delivers both benefits in a clean and elegant package—by leveraging best-in-class RF components, algorithms, and an industry-first cloud-managed security radio dedicated to monitoring the RF airspace to optimize performance.

Using the Cisco Meraki Dashboard and cloud-managed wireless APs, network admins can build a robust WiFi network capable of meeting the most demanding high-density needs and overcoming challenging RF interference environments. This whitepaper describes the underlying algorithms of the Cisco Meraki Auto RF, as well as the tools available for RF visualizations and customization in the Meraki dashboard.



□	Status ▲	Name	Channel
□	G ✓ 26	3 C4	11, 44
□	G ✓ 34	4 L9	11, 149
□	G ✓ 34	A2 C100 A	1, 48
□	G ✓ 34	A8 1720 A	1, 36
□	G ✓ 34	A10 1DD0 A	6, 149
□	G ✓ 34	B6 C190 A	11, 153
□	G ✓ 34	C4 C240 A	6, 161
□	G ✓	C7 1E20 A	11, 48

Figure 1: Cisco Meraki Auto RF engine automatically configures optimal channel plan

Cloud-based RF Analysis

In a challenging wireless network deployment, automatic interference detection and mitigation is a critical element to delivering high-performance WiFi. Out-of-the-box spectrum intelligence should be included as a part of any enterprise WiFi vendor's toolset. Cisco Meraki wireless products have built-in "Auto RF" algorithms for real-time data collection and channel optimization. This functionality is included with the baseline cloud license. Cisco Meraki wireless access points and the cloud architecture work in tandem to leverage real-time RF samples from the APs to create a comprehensive system of data aggregation and RF environmental computation. This data is collected along with signal strength and channel utilization data to build a cross-channel view of interference, from which optimal channel settings are chosen by the cloud servers and pushed to the edge devices. The inclusion of a dedicated security radio in the newer Cisco Meraki wireless platforms means that the Cisco Meraki cloud collects data in real-time across all channels, regardless of whether or not clients are being served from the primary radios.

Gathering RF data

Cisco Meraki APs continuously perform real-time spectral scanning, even whilst serving clients. Specifically, there are three types of scans that occur across all channels:

- **Spectral scans—**looking at pure RF data (in-phase and quadrature samples that produce Fast Fourier Transform-based spectral information; see section 3, "RF management tools")

- **Rogue scans—**looking for rogue SSIDs, used for the Air Marshal WIPS (see the Air Marshal whitepaper for more details)

- **Containment scans—**also used for Air Marshal rogue containment

The above scans are typically run across all channels on both the 2.4 GHz and 5 GHz channels once every 4 seconds, as approximately 33 channels (including DFS channels) are scanned for approximately 150 milliseconds each. While the user is viewing the live spectrum graphs (as described in Section 3), all spectral data is gathered within 1 second to paint a real-time cross-channel view.

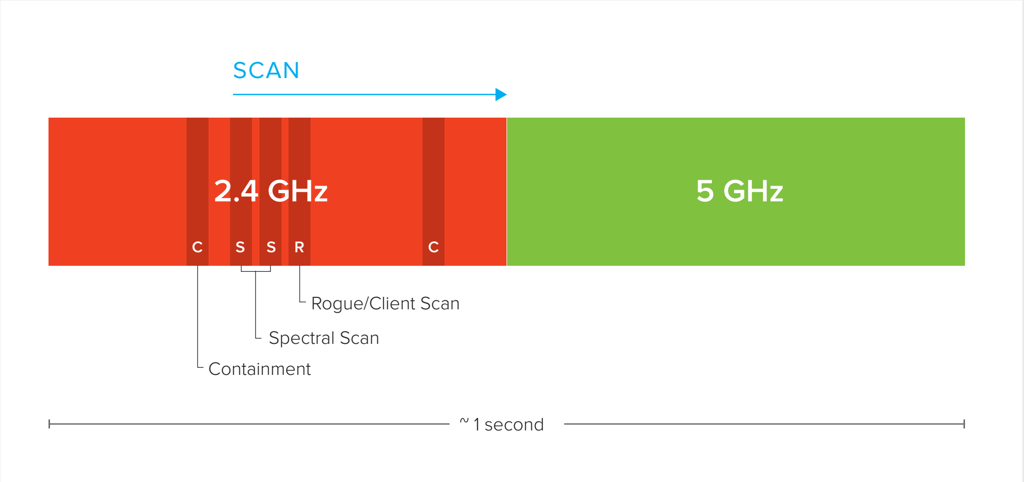


Figure 2: Cisco Meraki Auto RF channel scanning sequence

Auto RF: Computing the optimal channel plan

The Cisco Meraki security radio continuously gathers RF data in the AP's memory buffer; the data is batched and fed to the Cisco Meraki cloud every 2 minutes. The cloud analysis engine calculates a cost function for each channel to determine the cleanest RF channels:

Σ RSSI of each BSSID + % of time noise floor beyond certain threshold (channel utilization)

Figure 3: Cost Function - Summation of RF data for each channel

The cost function is computed by taking a sum of signal strength data from all neighboring APs in addition to channel utilization estimates. This data is computed separately for each channel during the security radio's scan. The algorithm then compares the data and selects the channel with the lowest value. On average, the cost function is updated every 10 minutes.

The calculation of the cost function drives the channel change logic of the wireless AP based on three main AP states:

1. **System bootup logic**—triggered when the AP first comes online. The AP scans the surrounding environment and feeds data to the Cisco Meraki cloud, which then determines the RF channel cost function for the AP within the first two minutes.

2. **Steady-state logic**—after the Cisco Meraki cloud chooses the best channels based on the system bootup cost function and the AP configures accordingly, it goes into a steady-state logic mode in which the AP sends RF data to the cloud every two minutes. In this state, the cloud runs the cost function algorithm every 10 minutes to identify if there are better channels for the AP. If the algorithm finds better channels, the AP moves to that channel if no clients are currently associated. If clients are associated, the Cisco Meraki AP will be sticky on the first channel so as not to interrupt the client application experience. If channel interference continues to increase beyond a noise threshold, the AP will enter the jammed-state logic.

3. **Jammed-state logic**—triggered when one or more devices operating on the APs steady-state channel cause channel utilization to exceed an acceptable noise threshold, rendering the channel unusable. In this case, the cloud computes a next-best channel for the AP to move to, and will momentarily disassociate clients as it switches to the lower-utilized channel.

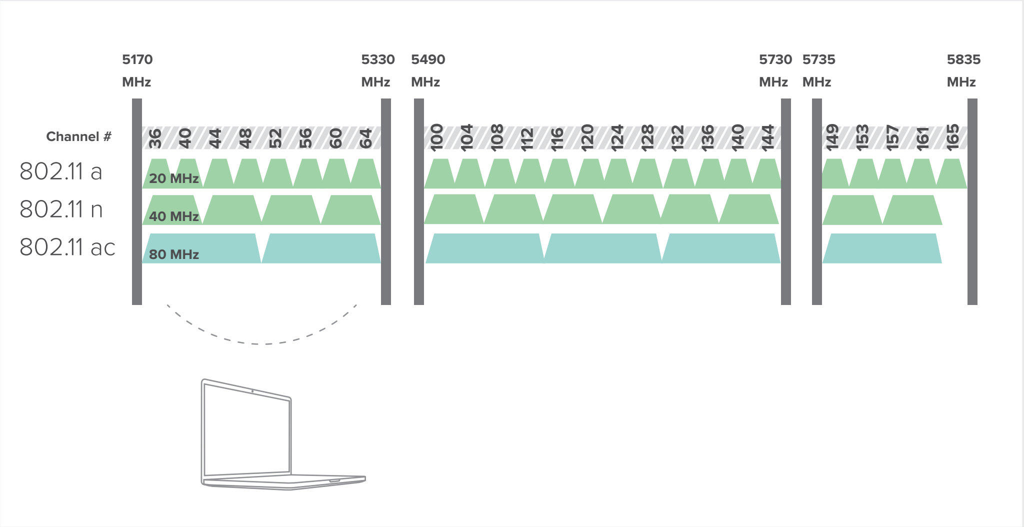


Figure 4: 802.11ac client changing channels on the 5 GHz band

During the channel change process, client performance is emphasized as much as possible; the overall goal of the wireless experience is stable client connectivity. As channel changes could disrupt less sophisticated wireless clients, channel changes are only undertaken when the RF interference has been determined to be high enough that the client experience is already rendered extremely ineffective (e.g., high latency whilst on VoIP, buffering during HD video streaming). This algorithm helps ensure that channel changes are minimally disruptive and that the client experience is optimized.

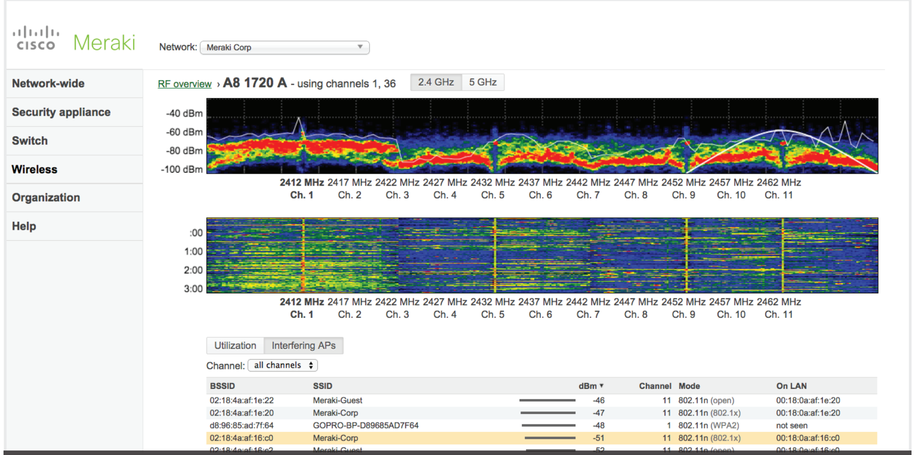
RF Management Tools

With increasing RF contention and proliferation of APs and devices, troubleshooting RF issues can sometimes be a hands-on experience. The Cisco Meraki Dashboard displays intuitive and insightful RF data that can be coupled with management tools for effective network planning. For RF visuals, the Cisco Meraki security radio gathers tens of thousands of RF samples and uses this to create FFT (fast fourier transform) and time-lapse RF spectrogram data graphs, enabling a truly granular and real-time view of the spectrum. For RF controls, the Cisco Meraki Dashboard includes a comprehensive set of RF controls overlaid on Google Maps and custom floorplans for visually intuitive fine-tuning.

Spectrum analysis data

Fast fourier transform (FFT) algorithms have been in widespread use for engineering and science applications to convert time-domain measurements to the related frequency-domain content (and vice versa). The Cisco Meraki security radio uses cross-channel spectral scans to gather thousands of RF samples per minute; this data is then used to plot frequency diagrams. For wireless applications, FFTs allow for visualization of energy across the 802.11 frequency bands, with colors indicating amplitude or density. There are two complementary visualizations, as seen in Figure 5:

- FFT density plot—the white line in the upper graph fluctuates in real-time and shows where the current signal energy levels are, which can be compared with different colors indicating the density of signals at a particular frequency over time (higher density signals are displayed in red, low density in blue).
- Time-lapse spectrogram—the second graph displays RF signal amplitude across the 802.11 frequency bands against time. Spectrograms can be helpful in determining how long a source of interference stayed on channel (e.g., a microwave running for 30 seconds vs. a continuous interference source from a 2.4 GHz wireless IP camera).


cisco Meraki
Network: Meraki Corp
Network-wide
Security appliance
Switch
Wireless
Organization
Help
RF overview › A8 1720 A - using channels 1, 36
2.4 GHz
5 GHz
-40 dBm
-60 dBm
-80 dBm
-100 dBm
2412 MHz 2417 MHz 2422 MHz 2427 MHz 2432 MHz 2437 MHz 2442 MHz 2447 MHz 2452 MHz 2457 MHz 2462 MHz
Ch. 1 Ch. 2 Ch. 3 Ch. 4 Ch. 5 Ch. 6 Ch. 7 Ch. 8 Ch. 9 Ch. 10 Ch. 11
:00
1:00
2:00
3:00
2412 MHz 2417 MHz 2422 MHz 2427 MHz 2432 MHz 2437 MHz 2442 MHz 2447 MHz 2452 MHz 2457 MHz 2462 MHz
Ch. 1 Ch. 2 Ch. 3 Ch. 4 Ch. 5 Ch. 6 Ch. 7 Ch. 8 Ch. 9 Ch. 10 Ch. 11
Utilization
Interfering APs

Channel: all channels

BSSID	SSID	dBm ▾	Channel	Mode	On LAN
02:18:4a:af:1e:22	Meraki-Guest	-46	11	802.11n (open)	00:18:0a:af:1e:20
02:18:4a:af:1e:20	Meraki-Corp	-47	11	802.11n (802.1x)	00:18:0a:af:1e:20
d8:96:85:ad:7f:64	GOPRO-BP-D89685AD7F64	-48	1	802.11n (WPA2)	not seen
02:18:4a:af:16:c0	Meraki-Corp	-51	11	802.11n (802.1x)	00:18:0a:af:16:c0
02:18:4a:af:16:c2	Meraki-Guest	-52	11	802.11n (open)	00:18:0a:af:16:c0

Figure 5: RF Spectrum page in Cisco Meraki dashboard

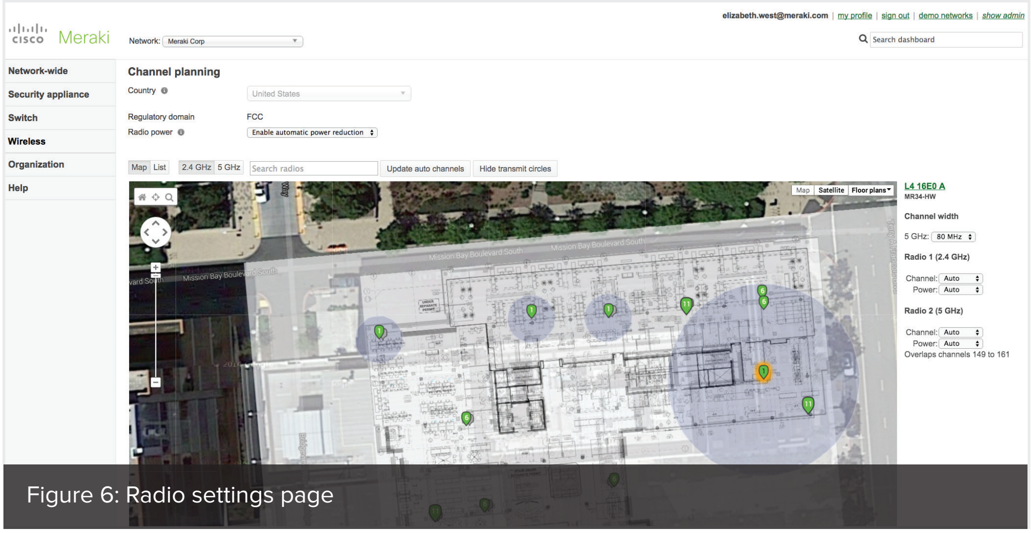
By using FFTs to understand real-time RF interference and patterns over time, the administrator has additional visual resources available for determining channel interference and then taking appropriate mitigating actions (e.g., moving an AP to a different channel or removing an interfering device).

Rogue data

As described in section 2, one of the three continuous scans is a rogue scan, used to compile a list of rogue SSIDs and their respective signal strengths. Rogue data collected via this mechanism is then displayed on the RF spectrum page and can be filtered by noise level and channel. Listed rogue access points can also be selected for visual overlay on the FFT. An understanding of the rogue AP distribution coupled with an understanding of interference on a particular channel can be utilized with the Cisco Meraki Air Marshal feature set to take measures for rogue containment and/or removal.

Visualization for easier RF management

In addition to the RF spectrum visual tools, the Cisco Meraki Dashboard also includes a radio settings control panel which can enable seamless RF changes in complex deployments. Settings include the ability to modify channel, power, and channel width (bonding) settings.



Network: Meraki Corp

Channel planning

Country: United States

Regulatory domain: FCC

Radio power: Enable automatic power reduction

L4 16E0 A
MR34-HW

Channel width

5 GHz: 80 MHz

Radio 1 (2.4 GHz)

Channel: Auto
Power: Auto

Radio 2 (5 GHz)

Channel: Auto
Power: Auto
Overlaps channels 149 to 161

Figure 6: Radio settings page

A note on channel bonding:

Channel bonding refers to the ability to manually choose 20, 40 or 80 MHz channels for communication between client devices and wireless APs. The defaults chosen for wireless communication by Cisco Meraki APs are 40 MHz and 80 MHz (for 802.11n and 802.11ac, respectively), which are the industry-wide standards. In rare cases, admins may want to restrict a channel to a narrower width by dropping it down to 20 MHz (e.g., in high-density deployments). These settings can be configured on a per-AP basis.

Additional tools

In addition to the radio settings page, a wide variety of other RF and Quality of Service (QoS) mechanisms are included in the Cisco Meraki Dashboard to assist in managing and optimizing RF performance. Examples include:

- **Band steering:** Enabling band steering allows the AP to steer clients from the 2.4 GHz to the 5 GHz band (if the client is 5 GHz capable). This helps free up airspace on the 2.4 GHz band, which has fewer channels and more co-channel overlap than the 5 GHz band.
- **Disabling legacy bitrates:** 802.11 clients exist in a wide variety of forms (802.11a/b/g/n/ac). Newer 802.11n and 802.11ac APs are designed to be backward-compatible with older clients conforming to the 802.11a/b/g standards. The problem is that these legacy clients are slower and take up more airtime—and can therefore cause performance degradation for faster clients. Disabling older bitrates could help solve performance issues for faster clients.
- **Layer 7 firewalling and QoS:** By using Cisco Meraki traffic analytics, it is possible to study the mixture of applications and traffic flowing across the network; this information can then be utilized for creating Quality of Service (QoS) policies to prioritize certain traffic (e.g., VoIP, video), traffic shape, or completely firewall other traffic (e.g., P2P filesharing). More details are available in the Cisco Meraki Layer 7 Visibility and Control whitepaper.

RF Management Today

The Cisco Meraki Dashboard provides unmatched visibility into devices, applications, presence and foot traffic, and now the RF airspace. Auto RF enables hands-off RF optimization, but provides more hands-on admins a complete and granular RF toolset for fine-grained administration. By using the powerful combination of a dedicated security radio, Auto RF optimization algorithms, and a comprehensive visual and administrative RF toolset, admins can fully leverage Cisco Meraki for real-time monitoring and management of an increasingly complex RF environment. In a time when there is increasing reliance on WiFi for mission critical applications and operations, network admins who deploy Cisco Meraki can now rest assured that they will have complete visibility and control of their RF, and will therefore be extremely well equipped to lead their next-gen WiFi deployments in the time of 802.11ac gigabit WiFi.