Managing and Optimizing RF Spectrum for Aruba WLANs

Version 1.0
Managing and Optimizing RF Spectrum for Aruba WLANs

Copyright

© 2012 Aruba Networks, Inc. AirWave®, Aruba Networks®, Aruba Mobility Management System®, Bluescanner, For Wireless That Works®, Mobile Edge Architecture®, People Move. Networks Must Follow®, RFprotect®, The All Wireless Workplace Is Now Open For Business, Green Island, and The Mobile Edge Company® are trademarks of Aruba Networks, Inc. All rights reserved. Aruba Networks reserves the right to change, modify, transfer, or otherwise revise this publication and the product specifications without notice. While Aruba uses commercially reasonable efforts to ensure the accuracy of the specifications contained in this document, Aruba will assume no responsibility for any errors or omissions.

Open Source Code

Certain Aruba products include Open Source software code developed by third parties, including software code subject to the GNU General Public License (“GPL”), GNU Lesser General Public License (“LGPL”), or other Open Source Licenses. The Open Source code used can be found at this site:

http://www.arubanetworks.com/open_source

Legal Notice

ARUBA DISCLAIMS ANY AND ALL OTHER REPRESENTATIONS AND WARRANTIES, WHETHER EXPRESSED, IMPLIED, OR STATUTORY, INCLUDING WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, NONINFRINGEMENT, ACCURACY AND QUIET ENJOYMENT. IN NO EVENT SHALL THE AGGREGATE LIABILITY OF ARUBA EXCEED THE AMOUNTS ACTUALLY PAID TO ARUBA UNDER ANY APPLICABLE WRITTEN AGREEMENT OR FOR ARUBA PRODUCTS OR SERVICES PURCHASED DIRECTLY FROM ARUBA, WHICHEVER IS LESS.

Warning and Disclaimer

This guide is designed to provide information about wireless networking, which includes Aruba Network products. Though Aruba uses commercially reasonable efforts to ensure the accuracy of the specifications contained in this document, this guide and the information in it is provided on an “as is” basis. Aruba assumes no liability or responsibility for any errors or omissions.

ARUBA DISCLAIMS ANY AND ALL OTHER REPRESENTATIONS AND WARRANTIES, WHETHER EXPRESSED, IMPLIED, OR STATUTORY, INCLUDING WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, NONINFRINGEMENT, ACCURACY, AND QUIET ENJOYMENT. IN NO EVENT SHALL THE AGGREGATE LIABILITY OF ARUBA EXCEED THE AMOUNTS ACTUALLY PAID TO ARUBA UNDER ANY APPLICABLE WRITTEN AGREEMENT OR FOR ARUBA PRODUCTS OR SERVICES PURCHASED DIRECTLY FROM ARUBA, WHICHEVER IS LESS.

Aruba Networks reserves the right to change, modify, transfer, or otherwise revise this publication and the product specifications without notice.
# Table of Contents

**Chapter 1: Introduction**  
Reference Material 5

**Chapter 2: Components of Aruba Spectrum Management Solution** 6  
**Aruba Solution: Theory of Operation** 6  
  Multi-purpose Access Points 8  
  Aruba Mobility Controllers 9  
  AirWave Management Platform (AMP) 10

**Chapter 3: Configuration of Spectrum Analysis** 11  
**Configuring APs for Spectrum Monitoring** 11  
  Configuring a dedicated spectrum monitor 11  
  Configuring a hybrid spectrum monitor 12  
  Provisioning APs in the correct AP Group 12  
**Navigating the Spectrum Dashboard** 13  
  Enabling RF Visualization 14  
**Integrating AirWave into the Network** 18

**Chapter 4: Understanding the Spectrum Charts and Usage** 20  
**Aruba’s Spectrum Analysis** 20  
**Using RF Signatures to Identify Interference Sources** 23  
**Recording and Playback** 25

**Chapter 5: Integration with AirWave** 26  
**Radio Statistics on AMP** 26  
**Issue Summary Section** 27  
**802.11 Radio Counters Summary** 27  
**Real Time RF Graphs** 28  
**ARM Event Logs** 28  
**Interfering Devices Table** 28  
**Active BSSIDs Table** 29  
**Spectrum Visualization using AMP** 29  
**Location Tracking of Interference Sources** 29  
**Integrated Real-Time RF Alerts** 30  
**Proactive RF Health Reports** 31
<table>
<thead>
<tr>
<th>Chapter 6: Example Use Cases</th>
<th>34</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Real-Time Troubleshooting with AirWave</strong></td>
<td>34</td>
</tr>
<tr>
<td>Example 1: Detecting, Classifying and Locating an Interference Source using Aruba WLAN</td>
<td>34</td>
</tr>
<tr>
<td><strong>Proactive Troubleshooting with AirWave</strong></td>
<td>40</td>
</tr>
<tr>
<td>Example 1: Too Many Channel/Power Changes</td>
<td>41</td>
</tr>
<tr>
<td>Example 2: High Channel Utilization on an Access Point</td>
<td>42</td>
</tr>
<tr>
<td><strong>Conclusion</strong></td>
<td>43</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Appendix A: Contacting Aruba Networks</th>
<th>44</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Contacting Aruba Networks</strong></td>
<td>44</td>
</tr>
</tbody>
</table>
Managing WLANs provides unique challenges not found in traditional LAN management. Unlike wired LANs, when there is a connection problem there is no wire to trace. The uncertainty associated with WLANs adds to the complexity in troubleshooting in the event of a performance issue. WLANs operate in “unlicensed” radio frequency (RF) spectrum and must co-exist with many other devices. These include microwave ovens, cordless phones, DECT headsets, Bluetooth devices, wireless gaming consoles, and video bridges. Each of these devices has the potential to interfere with the WLAN network. The characteristics and severity of interference varies depending on the type and the location of that device. It can be continuous or intermittent, at the campus or at the remote site. In addition to these disruptive non-802.11 sources of interference, adjacent channel and co-channel interference can also affect WLAN performance.

For WLANs to be able to reliably support mission-critical, high-throughput, or time-sensitive applications, RF interference must be continuously monitored. The WLAN must automatically and dynamically adapt to mitigate the effects of any interference in the environment. WLAN infrastructure has to provide the administrators with real-time, historical, and proactive visibility into the air to diagnose and mitigate interference. In this application note we will look at some of the tools that Aruba offers as a part of its WLAN solution that enable administrators to ensure reliable, high performing RF.

Table 1 lists the current software versions for this guide.

### Table 1 Aruba Software Versions

<table>
<thead>
<tr>
<th>Product</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>ArubaOS™ (Mobility Controllers)</td>
<td>6.1</td>
</tr>
<tr>
<td>ArubaOS (Mobility Access Switch)</td>
<td>7.0</td>
</tr>
<tr>
<td>Aruba Instant™</td>
<td>1.1</td>
</tr>
<tr>
<td>MeshOS</td>
<td>4.2</td>
</tr>
<tr>
<td>AirWave</td>
<td>7.3</td>
</tr>
<tr>
<td>AmigopodOS</td>
<td>3.3</td>
</tr>
</tbody>
</table>

### Reference Material

- This guide assumes a working knowledge of Aruba products. This guide is based on the network detailed in the Aruba Campus Wireless Networks VRD and the Base Designs Lab Setup for Validated Reference Design. These guides are available for free at http://www.arubanetworks.com/vrd.

- The complete suite of Aruba technical documentation is available for download from the Aruba support site. These documents present complete, detailed feature and functionality explanations outside the scope of the VRD series. The Aruba support site is located at: https://support.arubanetworks.com/. This site requires a user login and is for current Aruba customers with support contracts.
Chapter 2: Components of Aruba Spectrum Management Solution

This chapter focuses on the various components of the Aruba WLAN network and the role that they play in identifying and troubleshooting performance related issues.

Aruba Solution: Theory of Operation

Interference in 802.11 WLANs is both inevitable and unpredictable. It varies by device (microwave, cordless phone), usage pattern (time variance), and location (local emissions regulations, construction). It must be managed to ensure reliable Wi-Fi operation. This calls for an integrated feature set that constantly monitors the RF environment for poor channel quality, optimizes the RF without manual intervention and offers visibility into the air with intuitive troubleshooting tools.

Aruba’s channel quality aware Adaptive Radio Management (ARM) technology boosts reliability and performance, leveraging infrastructure-based controls to enhance overall network performance for wireless deployments. Adaptive RF scanning on all Aruba APs ensures that the controller is aware of the instantaneous interference and coverage indices. The indices includes the non Wi-Fi duty cycle, noise floor, retries over the air and PHY errors. ARM uses this intelligence to take necessary actions to restore performance in the affected area. Moreover infrastructure control features such as band steering, spectrum load balancing and airtime fairness boosts overall network performance by balancing clients equitably. The resulting user experience is a reliable high performing network that makes the shared medium less like a hub and more like a switch.

In most WLAN deployments the primary source of any performance degradation starts at layer 1 i.e. at the RF spectrum or physical layer. Aruba offers integrated spectrum analysis, which adds a layer of visibility into 802.11 WLANs. Visibility into the RF allows the network engineer to see what is occurring in the air and is a key requirement for troubleshooting such issues. Spectrum analysis can classify and identify non-802.11 interference sources, providing real-time analysis at the point where the problem occurs. It is best utilized as integrated into the WLAN infrastructure since hand-held tools are useful only when IT staff are on-site and interference is present – an unlikely combination in distributed enterprises. The solution to the problem is a set of integrated tools that enable visibility from using the existing infrastructure. As shown in Figure 1, the Aruba product set of mobility controllers and APs work together to scan and report on sources of interference.

![Figure 1](image_url)

**Figure 1**   Spectrum Analysis with Aruba Mobility Controllers and APs
Aruba combines the capabilities of the AP’s hardware spectrum analysis functionality with ArubaOS software to enable the detection and classification of both 802.11 and non-802.11 sources of interference. APs scan the environment and feed the information to the Aruba Mobility Controller. The controller is equipped with a fully integrated spectrum analysis dashboard shown in Figure 2. This dashboard provides RF visualization information.

As shown in Figure 3 below, the AirWave management platform (AMP) is Aruba’s unique management solution that integrates configuration, management, and troubleshooting for both wired and wireless devices for a multi-vendor network in a single appliance. It offers complete integration with ARM statistics and integrates with the spectrum analysis dashboard hosted by the Aruba Mobility Controller for visualization. In addition, real-time RF alerts inform the administrator when there is an issue, trending and historic RF information enable forensic analysis, and RF health reports aid in proactive planning.
The following components make up the Aruba integrated solution to provide visibility into RF:

1. Multi-purpose Access Points
2. Aruba Mobility Controller with the RFProtect™ license
3. AirWave Management Platform (AMP)

**Multi-purpose Access Points**

Aruba 802.11n access points are based on the Atheros XSpan technology. The Wi-Fi chipset from Atheros was developed from the ground up with integrated high definition spectrum analysis capabilities as one of the core objectives. With a custom-built processor and a dedicated TPM, Aruba’s 802.11n AP platforms are capable of performing multiple operations without compromising security and without added costs. There are three modes of operation for an Aruba AP, they are hybrid, air-monitor and spectrum monitor respectively. Let us look at the different operating modes of an Aruba AP in more detail.

**Access Point (AP) mode**

When the AP is operating in the AP mode, it will serve clients and go off-channel periodically to scan the RF environment for assessing the RF neighborhood. It can also gather IDS events, perform rogue detection and perform rogue containment in this mode. Although the AP does not perform any spectrum scanning in this mode, it will still monitor the interference and coverage indices in the environment. When interference crosses a certain threshold, Aruba’s adaptive radio management (ARM) technology, which is integrated into the base ArubaOS, adapts and selects a better channel in order to maintain reliable RF.

**Hybrid AP mode**

When the radio is in the AP mode with Spectrum Monitoring enabled, it will serve clients and go off-channel periodically to scan the environment for security events, similar to the previous mode. In addition, it also performs spectrum scanning on the “home channel” which is the channel of operation for the AP radio. This will allow the radio to detect and classify interference sources and send the classification information to AirWave for aggregation and reporting. Moreover, it will also display the spectrum charts for RF visualization on the home channel.

**Air Monitor (AM) mode**

When the radio is in the air monitor mode its functionality is limited to wireless IDS event detection, rogue detection and containment. It spends 100 percent of the time scanning channels in the configured domain and does not perform any kind of spectrum scanning.

**Spectrum Monitor (SM) mode**

When the radio is in a spectrum monitor mode its primary responsibility is to perform spectrum scanning across the entire band of operation. This data is then fed up to the Aruba Mobility Controller and AirWave. The APs also scans for wireless IDS event detection, rogue detection and containment, but it does not serve clients in this mode.

Aruba has a broad portfolio of access points that provide a lot of flexibility for customers to pick and choose the best product that satisfies their network requirements. All Aruba access points are “noise aware”, which means that they have the capability to detect an RF anomaly and select a better channel. Moreover, most Aruba 11n APs are capable of classifying noise sources. Table 2 lists out all
Aruba APs and the supported modes of operation for each.

### Table 2  AP Spectrum Capability

<table>
<thead>
<tr>
<th>Device</th>
<th>Configurable as a Spectrum Monitor?</th>
<th>Configurable as a Hybrid AP?</th>
</tr>
</thead>
<tbody>
<tr>
<td>AP-105</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>AP-90 Series</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>AP-120 Series</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>AP-130 Series</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>AP-175</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

### Aruba Mobility Controllers

The Aruba Mobility Controller is a key component of the solution that enables granular visibility into the RF. The APs scan the air for spectrum related events, detect and classify interference. They feed this information to the mobility controller that aggregates spectrum data from multiple spectrum analysis capable APs. This spectrum intelligence is used by the Adaptive Radio Management (ARM) technology to build the RF neighborhood table so that it knows which channel to move to when the air quality crosses a certain threshold. The spectrum dashboard housed by the Aruba Mobility Controller provides the in-depth RF visualization.

The Aruba spectrum analyzer is available on ArubaOS release 6.0 and newer. This means it is supported on Aruba 600 Series, Aruba 3000 Series, and Aruba 6000 Mobility Controllers. The feature can be enabled with the RFPprotect license on the Aruba Mobility Controller. The number of spectrum sensors supported by a controller varies on a per-controller basis, and is equal to the number of APs that can be supported by a particular controller model. Table 3 lists the number of spectrum monitors supported by each controller model.

### Table 3  Spectrum Monitor Count per Mobility Controller

<table>
<thead>
<tr>
<th>Controller Model</th>
<th># of spectrum monitors supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aruba 6000 Chassis (4x M3s)</td>
<td>2048</td>
</tr>
<tr>
<td>M3 Supervisor Card</td>
<td>512</td>
</tr>
<tr>
<td>Aruba 3200XM/Aruba 3400/Aruba 3600</td>
<td>32/64/128</td>
</tr>
<tr>
<td>620 Controller/650 Controller/651 Controller</td>
<td>8/16/16</td>
</tr>
</tbody>
</table>

Note that the Spectrum dashboard (UI) is integrated with ArubaOS WebUI housed by the Aruba Mobility Controller, which is typically accessed from the management station. Aruba allows more than one Spectrum monitor to be connected to a single UI client instance. However, the maximum number of simultaneous SMs that can be connected to a single UI client will be limited by the capabilities of the client, including the CPU and memory. As a rule of thumb, expect a given client to support up to six SMs. Additionally, the number of simultaneous client UI sessions per controller is limited to 20.
AirWave Management Platform (AMP)

AMP is the ideal management platform for monitoring the entire wireless LAN to maintain robust performance and deliver an optimal wireless experience to mobile end users. AMP acts as a centralized network management system that aggregates the interferer information across the network. In addition to the instantaneous interferer information, AMP offers historic information that enables debugging and troubleshooting performance-related issues with more context. The information ranges from interference detection, classification of interferes, the channels affected by interference, the duty cycle of the interferer, and the timestamp when the interferer was detected. AMP also integrates location tracking of the interfering device adding more context into performance issues. In addition to detailed interference related information, AMP offers pre-defined, custom RF health reports that act as a proactive tool to identify and isolate problem devices on the network. Real time alerts inform the administrators of an issue before a helpdesk ticket is logged, thereby enabling more efficient troubleshooting. For detailed RF visualization, AMP has a quick link to the spectrum dashboard hosted by the WLAN controller.
Chapter 3: Configuration of Spectrum Analysis

This chapter focuses on setting up the Aruba WLAN for spectrum analysis. The first steps will be configuring APs, followed by mobility controllers, and then the AirWave platform.

Configuring APs for Spectrum Monitoring

This section covers the various ways to make an Aruba AP ready for spectrum analysis, which includes dedicated spectrum monitoring and hybrid spectrum monitoring.

Configuring a dedicated spectrum monitor

A dedicated spectrum monitor is setup to only monitor the RF environment. This station can be configured individually, but it is more common to have an AP group dedicated to spectrum monitoring that shares similar configuration. In order to create a spectrum-monitor group navigate to the AP group configuration page at configuration > AP Configuration and select new in the AP group page to define the name of the spectrum-monitor group as shown in the Figure 4.

Once the group has been defined, navigate to the AP radio profile at Configuration > AP Configuration > spectrum-monitor > RF Management > Radio profile and select the “spectrum-mode” as the mode of operation as shown in Figure 5.
Configuring a hybrid spectrum monitor

A hybrid spectrum monitor serves clients and provides spectrum analysis details at the same time. As explained earlier it is a recommended best practice to define a separate AP group for hybrid APs, so that the APs in the network can share the same configuration. Using the same radio profile that was referenced earlier, select ‘ap-mode’ for the mode of operation as shown in Figure 6. In the lower left hand corner check the ‘spectrum monitoring’ checkbox to activate spectrum scanning on the home channel.

![Figure 6 Configuring a Hybrid AP](image)

Provisioning APs in the correct AP Group

A new AP that comes up for the first time has to be manually provisioned in the correct AP group. Once provisioned the AP downloads its configuration from the controller and becomes functional. This is typically a one-time process that instructs the AP the group that it belongs to. In order to provision an AP, navigate to configuration > AP Installation. Select the AP that needs to be provisioned and then select provision as shown in Figure 7 below. In the provisioning page, ensure that the AP has a name and AP group as intended. The AP will reboot and come up again as part of the AP group that it was configured to be in.

![Figure 7 AP Provisioning in the Configuration Tab](image)
Navigating the Spectrum Dashboard

An intuitive graphical user interface with drop-down selection options and vivid color charts makes it simple to set up and to use the spectrum analyzer module on the Aruba Mobility Controller. A spectrum dashboard is divided into two areas, the title bar and the chart area. As seen in Figure 8 below, the top most pane in the dashboard is the title bar. It shows three tabs – view 1, view 2, view 3 and recording/playback. Each view lets you display 4 different charts. The bottom pane is known as the chart area, which can display the different charts such as the FFTs, Spectrograms, active devices etc. Aruba offers a variety of built-in charts that the administrators can select for each view.

Figure 8    Spectrum Dashboard
Enabling RF Visualization

The following steps detail the process of connecting to a SM and displaying graphs and charts of the RF environment.

1. In order to enable visualization the AP radios that are required to perform spectrum analysis need to be manually connected to. On the controller WebUI navigate to the spectrum analysis section under the monitoring tab. A new window will pop up. As shown in Figure 9 navigate to the spectrum monitors tab and select the radios that you want to fetch visualization data from. Select the appropriate radio that you want to connect to and click connect. The spectrum dashboard will get populated for the selected spectrum monitors.

![Figure 9 Connecting to a Spectrum Monitor](image_url)
2. The amount of information provided by a spectrum dashboard depends on the AP’s mode of operation. A dedicated spectrum monitor gives a real-time snapshot across the entire spectrum for a particular AP radio as shown in Figure 10 below.

Figure 10  Spectrum Dashboard for a Spectrum Monitor in the 2.4 GHz Band
3. The spectrum dashboard for a hybrid AP will give a real-time snapshot for the home channel as shown in the Figure 11. In the upcoming section we will talk more about the spectrum dashboards, the charts and what each chart means to a WLAN administrator.

If you look at the chart area as shown in Figure 12 there are three arrows on the top right corner of each chart. Click on the right-most arrow for a dropdown of available spectrum monitors. This section assumes that the spectrum monitors have already been added to the spectrum dashboard based on the configuration steps provided earlier.

Figure 11  Spectrum Dashboard for a Hybrid AP on Channel 11

Figure 12  Spectrum Chart Drill Down
The middle arrow allows the user to maximize and restore a chart. The user can tunnel down into most charts to extract additional information. In the Figure 13 as shown below active devices and their associated configuration menus are presented.

![Figure 13 Active Devices Maximized View](image)

4. The right most arrows offer a few selectable parameters which are listed below:
   - **Options** – This brings up the options associated with each chart as described in the following sections.
   - **Replace with** – Shows a drop down of the different charts that can be reviewed.
   - **Help** – Provides basic information on the chart under display.
Integrating AirWave into the Network

In order to integrate AirWave into the system there are a few configuration steps involved. Navigate to Configuration-> Management and select SNMP. Define the SNMP system group parameters as shown in Figure 14 below. Most importantly the community string needs to match at the controller and the AirWave management platform for successful communication.

![SNMP System Group Configuration on the Aruba Mobility Controller](image)

On the same SNMP configuration page the AMP server needs to be added as a trap receiver with the appropriate parameters like the IP address, SNMP version, the community string, port type etc. as shown in Figure 15 below.

![SNMP Trap Receiver Configuration on the Aruba Mobility Controller](image)

In order to feed monitoring data from the controller to AirWave, the IP address needs to be added to the Aruba Mobility Controller as the management server. This configuration is done at the controller CLI. SSH into the controller and enter the “enable” mode, and issue the following command as shown below.

```
(Controller-Name) (config) # mgmt-server type amp primary-server <AMP IP>
```
The Aruba Mobility Controller is ready to send information to the AirWave server. As the final step in the configuration process the AirWave platform needs to know device it will be monitoring. AMP uses the Aruba topology to discover and monitor the infrastructure downstream. As long as the mobility controller is added to the system, AMP automatically detects the APS and the associated clients. The master controller can be either discovered from AMP, or added manually. Navigate to Device Setup->Add for manually adding the controller as shown in Figure 16 below. Enter the name, IP address and the community string of the controller. Ensure that the community string is the same as what you configured on the WLAN controller.

Within a few minutes after adding the controller, the AP and the associated client monitoring data will get populated on the AMP server. This ensures complete visibility into your network.
Chapter 4: Understanding the Spectrum Charts and Usage

In this section we will look at how this solution is integrated with AirWave network management system, and the detailed information that it offers for root cause analysis of a performance issue.

Aruba’s Spectrum Analysis

The spectrum analysis charts offered by Aruba’s solution can be broadly classified into three areas:

- **Active Devices Summary** - Active Devices by Device Type, Active Devices by Channel, Active Devices Trend
- **Channel Health** - Channel Metrics, Channel Quality Trend, Device Duty Cycle, Channel Utilization Trend
- **Interference Classification** - FFT Power, FFT Duty Cycle, Interference Power, Swept Spectrogram, Channel Quality Spectrogram

Below we will take a look at some of the charts and the relevance of each to a WLAN administrator.

<table>
<thead>
<tr>
<th>Chart Description</th>
<th>Visual Representation of the chart</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Active Devices</strong></td>
<td><img src="image.png" alt="Pie Chart" /></td>
</tr>
<tr>
<td>A pie-chart view of the Wi-Fi and non-Wi-Fi devices that are found on any given spectrum.</td>
<td></td>
</tr>
</tbody>
</table>

| **Devices vs. Channel** | ![Bar Chart](image.png) |
| This chart breaks up the active devices chart on a per-channel basis (Wi-Fi and non-Wi-Fi). |

| **Device Duty Cycle** | ![Bar Chart](image.png) |
| This chart provides a snapshot of channels that are heavily utilized and the ones which are not based on Wi-Fi and non-Wi-Fi devices. |
Active devices table
A table that lists all uniquely identified interferers and the associated ‘channels affected’.

Active Devices Trend
This chart provides a trend of the number of devices – both Wi-Fi and non-Wi-Fi seen on each channel over a snapshot of time.

Channel Metrics
This chart provides a snapshot of the Wi-Fi and non-Wi-Fi utilization for every channel in the spectrum.

Channel Metrics Trend
This chart provides a history of channel quality over a time range based on factors such as channel utilization, noise floor, error rate and retry rate.
Chart Description | Visual Representation of the chart
--- | ---
**Channel Summary Table**
This chart lists the valid and unknown APs, non-Wi-Fi devices and the signal to noise ratio (SNR) across the spectrum.

| Channel Utilization Trend | This chart gives a snapshot of the channel utilization over an interval of 10, 30 and 60 minutes.

| Real Time FFT | This chart plots the energy detected by the spectrum sensor at each frequency component in the specified range. This chart represents the strength of the noise source.

| FFT Duty Cycle | This chart displays the percentage of time that an interferer is active. This lets you estimate the impact of the interferer on the channel.
## Chart Description

<table>
<thead>
<tr>
<th>Chart Description</th>
<th>Visual Representation of the chart</th>
</tr>
</thead>
<tbody>
<tr>
<td>Swept Spectrogram</td>
<td><img src="image" alt="Swept Spectrogram" /></td>
</tr>
<tr>
<td>This chart is a color coded view of the real-time FFT, which indicates the strength of the interference. Blue to green is good or acceptable, whereas yellow, orange and red lead to poor WLAN performance.</td>
<td></td>
</tr>
</tbody>
</table>

| Quality Spectrogram | ![Quality Spectrogram](image) |
| This is a color coded chart that shows the channel quality over a period of time. Blue or green indicates good performance, while yellow, orange and red will lead to suboptimal WLAN performance. |

### Using RF Signatures to Identify Interference Sources

Each source of RF radiation is unique. The radiation from a source can be differentiated based on four factors:

- a. The frequency at which the interfering source is emitting
- b. The bandwidth occupied by the emission
- c. The strength of the radiation at each of the frequencies in (1) and (2)
- d. The percentage per unit time for which the source emits

These four parameters also determine the impact that the interference source would have on a WLAN operating in the same RF space. For example, a wide-band source radiating with high duty cycle and high amplitude will impact the WLAN adversely across a broad range of channels. A narrow-band source radiating with high amplitude, but away from the center frequency on which the AP is operating will have less of an impact.

These identifying characteristics can be learned primarily from information provided in two of the spectrum charts:

- a. Real time FFT chart
- b. FFT Duty Cycle Chart
Below are a few examples illustrating how different sources of WLAN interference would appear on these charts. By identifying RF signatures an administrator can proactively pinpoint interference sources and their impact in the environment.

<table>
<thead>
<tr>
<th>Description</th>
<th>RF Signature</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ambient Channel Condition shows no activity on the channel.</td>
<td><img src="image1.png" alt="Graph" /></td>
</tr>
</tbody>
</table>
| Signature of an AP  
The AP is operating on channel 1 and is heard by the spectrum monitor at -20 dBm (very close to the spectrum monitor). The spectrum extends strongly through channel 4 and then rapidly drops off. | ![Graph](image2.png) |
| Signature of a fixed frequency cordless phone.  
The device is operating on channel 1, the duty cycle of the device is usually on the order of 100%, which means that the emission is continuous and channel 1 is rendered unusable. | ![Graph](image3.png) |
| Signature of a frequency hopping device.  
The interferer hops from frequency to frequency across the entire 2.4 GHz spectrum. This is very disruptive as the AP will find it difficult to locate a clean channel. | ![Graph](image4.png) |
Recording and Playback

In the event that a network administrator gets periodic complaints of bad Wi-Fi performance at a particular time of the day, the recording/playback functionality allows the administrator to record the spectrum analysis information, store it on a local machine and replay it at a later time for post-analysis. As shown in Figure 17 the record and playback options offered by Aruba spectrum analysis are as follows:

a. Click on Record/Playback button which is located at the top right corner of the title bar.

b. Click on Make a New Recording.

c. Select the required spectrum monitor and select parameters on starting time and duration/size of the capture. Click OK. This starts the recording.

d. Once the desired event is captured, click on stop to terminate the capture earlier than configured.

Select the location to save the capture file. This creates a .sfr file with the monitor-name and band of operation in the file-name. To play back the file, click on Record/Playback and then ‘load playback file’. Browse the local machine to select the .srf file, and click on the green button to start the playback. The spectrum analysis tool allows you to record up to 60 continuous minutes (or up to 10 MB) of spectrum analysis data. By default, each spectrum analysis recording displays data for the Real-Time FFT, FFT Duty Cycle, and Swept Spectrogram charts, however, you can view device data for any the spectrum analysis charts supported by that spectrum monitor radio.
Chapter 5: Integration with AirWave

Radio Statistics on AMP

AMP has inherited the RF intelligence that an Aruba Mobility Controller has leveraging ARM technology, and provides the information in an intuitive graphical format that helps an administrator to understand the RF environment and take corrective action as required. Search for the desired AP in the network by typing its name on the AirWave search bar. Once AirWave locates the AP of interest, select the AP to navigate to the AP monitoring page. Select either one of the radios under the AP monitoring page as shown in Figure 18 to go to the individual radio statistics page.

![Figure 18 Radio Selection under the AP Monitoring Page](image)

![Figure 19 Radio Statistics Page on AMP](image)
Issue Summary Section

The issue summary section provides information pertaining to the noise floor, user count, interfering devices, channel utilization, bandwidth, MAC and PHY errors. This section informs the administrator that there is an issue, it helps identify what the issue is and isolates the cause for the issue. The default triggering thresholds for an issue summary is as follows:

<table>
<thead>
<tr>
<th>Issue</th>
<th>Triggering Threshold</th>
</tr>
</thead>
<tbody>
<tr>
<td>High Noise</td>
<td>-80</td>
</tr>
<tr>
<td>High number of Users</td>
<td>15</td>
</tr>
<tr>
<td>High Channel Utilization</td>
<td>75%</td>
</tr>
<tr>
<td>High Bandwidth</td>
<td>75% of max</td>
</tr>
<tr>
<td>Interfering Devices Detected</td>
<td>Detected within the last 5 minutes</td>
</tr>
<tr>
<td>High MAC/PHY Errors</td>
<td>1000 frames/sec</td>
</tr>
</tbody>
</table>

A typical issue summary section on the radio statistics page is shown below in Figure 20.

![Issues Summary](Figure 20)

802.11 Radio Counters Summary

This table provides visibility into the 802.11 counters and summarizes the number of times an expected acknowledgement frame was not received, the number of duplicate frames over the air, the number of frames with FCS errors, and the number of retries and failures. These are all symptoms of poor air quality which could have been caused due to issues such as 802.11 and non 802.11 interference, a busy RF environment with a lot of activity over the air, collisions, an older driver version on the client device, etc. A typical 802.11 radio counter summary is shown below in Figure 21.

![802.11 Radio Counters with Historic Data](Figure 21)
Real Time RF Graphs

Time series graphs for the radio are displayed across a tabbed, dual-pane interface to show changes recorded at different polling intervals over time. These are real-time graphs that provide a snapshot of the RF environment with historic information up to a year. Some of the relevant RF-related graphs are channel, noise, and power, 802.11 counters and channel utilization. In addition, these graphs also provide user and bandwidth related information for a particular radio. A typical radio statistics graph on AirWave is shown below in Figure 22.

![Radio Statistics Graphs with Historic Data](image)

**Figure 22** Radio Statistics Graphs with Historic Data

ARM Event Logs

This table lists the ARM-initiated events such as automatic channel changes, power changes, and mode changes. One valuable piece of information that this table provides is the specific reason for the ARM change as shown in Figure 23.

![ARM Event Logs with Change Reasons](image)

**Figure 23** ARM Event Logs with Change Reasons

Interfering Devices Table

For Aruba APs running either in hybrid or spectrum mode, the same non-802.11 interfering devices identified in the issues summary section are classified in the detected interfering devices table along with the timestamp of its last detection, the start and the end channel of the interference, the signal to noise ratio (SNR) and the duty cycle of the interferer as shown in Figure 24.

![Detected Interfering Devices Table](image)

**Figure 24** Detected Interfering Devices Table
Active BSSIDs Table

The table lists both the BSSID and the SSID detected by the AP radio on its channel of operation as seen in Figure 25. This provides the administrator with an indication of the degree of 802.11-based co-channel interference in the RF environment.

![Figure 25: Active BSSIDs Table](image)

Spectrum Visualization using AMP

In addition to the RF statistics that AMP provides, it also offers RF visualization by providing a quick link to the spectrum analysis dashboard for an in-depth analysis of non-802.11 sources of interference. This launches the spectrum dashboard without the need for additional software or hardware component thereby increasing the ease of troubleshooting for a WLAN administrator. The steps to launch the spectrum dashboard from AirWave are as follows:

- Search for the desired AP in the network by typing its name on the AirWave search bar.
- Once AirWave locates the AP of interest, select the AP to navigate to the AP monitoring page.
- The AP monitoring page provides a quick link to the spectrum dashboard as shown in Figure 26.

![Figure 26: Spectrum Dashboard Integration from AMP](image)

Location Tracking of Interference Sources

To provide more context for issues that are occurring on your wireless network, you need to know where your users and devices are located, and you need to monitor the RF environment in those areas. The visual RF (VRF) module in AMP provides a real-time picture of the live radio environment of your wireless network. In order to provide RF visibility, AMP uses sophisticated RF fingerprinting technology and compares the interference sources reported from multiple access points to triangulate the location of the interferer. Once the interfering devices have been located, it makes it possible for Visual RF to display the location of the interferer. Location tracking is integrated into the network management system, does not require any additional configuration, hardware appliances, or associated licenses.
Integrated Real-Time RF Alerts

AMP monitors certain key aspects of the air quality in the network. When certain parameters or conditions arise that are outside of normal operating conditions, AMP generates alarms that gives a real-time view of the network. This helps the administrator address the problem before users have a chance to report it.

Perform the following steps to configure and create a channel utilization trigger:

1. To create a new trigger, navigate to the Systems-> Trigger page and select the Add New Trigger button.

2. In the trigger type choose the ‘channel utilization’ trigger with a desired severity level. AMP uses certain matching conditions such as the radio type, interference, time busy, transmit time and receive time to determine the quality of air in the network as seen on Figure 27.

3. AMP monitors these conditions for duration of time to differentiate between persistent and transient issues.

4. Once the matching conditions are met AMP sends an email notification to the administrator in real-time.

![Channel Utilization Trigger on AMP](image_url)
**Proactive RF Health Reports**

AMP has developed reports for uniquely tracking the RF environment in a given deployment and identifying issues. AMP offers both custom and built-in RF health reports for ease of use. The built-in RF health report tracks the top AP radios by noise, MAC/PHY errors, channel changes, transmit power changes, mode changes and interfering devices. In addition, it assists in pinpointing the most problematic devices on your network and lists the top 10 devices by problem type. Custom health reports can be defined with a few key parameters that are of interest to the administrator.

Perform the steps mentioned below to configure one such report for your network:

1. Navigate to Reports -> Definition page and select the ‘add’ button. This will allow you to define a custom report using the ‘Custom Options’ drag and drop interface as shown in the Figure 28.

![Report Definition Page – Building Custom Reports](image)

2. AMP also has several built-in reports that an administrator can select. To view one such example select the pre-defined RF health report under the ‘type’ menu.
3. For either report option, AMP enables scheduling report in which the report can be run once or over a period of time. The generated report can be emailed to the administrator proactively. The configuration knobs are seen in Figure 29.

![Report Definition Page – Using Built-in Reports](image-url)

Figure 29  Report Definition Page – Using Built-in Reports
As explained earlier a typical RF health report has multiple fields of information. Selecting a field under the Device column in any table will take you to the APs/Devices > Monitor > Radio Statistics page for the band indicated in the table title (5 GHz or 2.4 GHz). A typical RF health report is shown in Figure 30.

![Figure 30 RF Health Report](image)

The table below lists the various fields included in a typical RF Health report and a brief description of what they mean to a WLAN administrator.

<table>
<thead>
<tr>
<th>Fields (2.4 and 5 GHz bands)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Problem devices</td>
<td>What are the problem radios in my network? A radio appears in this list only if it is listed in two other categories in this report. This list informs the administrator that the radios in this list require immediate attention.</td>
</tr>
<tr>
<td>Most Noise</td>
<td>Radios that are affected by irregular amounts of non-802.11 noise.</td>
</tr>
<tr>
<td>Most interfering devices</td>
<td>Radios that are affected by multiple sources of interference. This table lists the classified interference sources as seen by the radio.</td>
</tr>
<tr>
<td>Least utilized by channel</td>
<td>Radios that are least utilized by clients.</td>
</tr>
<tr>
<td>Most utilized by channel</td>
<td>Radios that are heavily utilized in terms of client traffic.</td>
</tr>
<tr>
<td>Most MAC/PHY errors</td>
<td>Radios that are experiencing irregular amounts of MAC/PHY errors which could be because of poor air quality.</td>
</tr>
<tr>
<td>Most channel changes</td>
<td>Radios that have maximum number of channel changes.</td>
</tr>
<tr>
<td>Most transmit power changes</td>
<td>Radios that have maximum number of power changes.</td>
</tr>
<tr>
<td>Most mode changes</td>
<td>Radios that have maximum number of mode changes (AP mode to monitor mode; and vice versa).</td>
</tr>
</tbody>
</table>
Chapter 6: Example Use Cases

In this section we will look at how the tools mentioned in the earlier sections can be used to perform real-time and proactive troubleshooting of RF related issues.

Real-Time Troubleshooting with AirWave

Example 1: Detecting, Classifying and Locating an Interference Source using Aruba WLAN

In this example, we have 3 x hybrid AP-135s named 135-1, 135-2 and 135-3. Since these are hybrid APs, they will serve clients and perform spectrum analysis simultaneously. These APs have a few clients associated to them. The APs are all terminating on an Aruba 3600 Mobility Controller. The APs and the WLAN controller are being managed by the AirWave management platform.

In the presence of a high duty cycle noise source like a video bridge, the client’s performance suffers. How does an Aruba WLAN help to identify and troubleshoot the issue in real-time?

1. A channel utilization trigger has been configured on AMP that generates an email notification to the WLAN administrator in the event of poor air quality.

2. In this scenario AMP has been configured to generate an email notification for a compound matching condition. The condition is as follow - the non 802.11 interference detected must be over 5% of the available channel, the channel utilization is more than 5%, and the interference source is observed for a minimum duration of 1 minute as shown in Figure 31.

![Channel Utilization Trigger for Real-time Alarms](image-url)
The noise source used in this example is a wide band fixed frequency noise source. A video bridge is a high duty cycle noise source (~ 90%) that operates over a range of frequencies in its band of operation (2.4 or 5 GHz). The air quality in the RF neighborhood will be impaired, which will affect the user experience adversely.

It is important to note that Adaptive Radio Management (ARM) will detect poor channel quality in the presence of the video bridge and dynamically pick a better channel. The video bridge is a wideband noise source however, and thus affects all the usable channels in the 2.4GHz band.

The hybrid AP-135s are constantly scanning for non-802.11 sources of noise and other wireless security events in the home channel, and also perform off-channel scanning at a regular interval. The AP is able to detect a high noise floor and feed that RF information to the Aruba Mobility Controller. The AP also detects and classifies the noise source. The controller is able to take this information from the AP and display it in the form of charts for visualization. The WLAN controller feeds this information to the AMP management system. When the matching channel utilization conditions configured on AMP are met, it automatically generates an email notification to the WLAN administrator.

Upon drilling down into the alert that the WLAN administrator has just received, some of the information that AMP has provided is included in the alert as shown in Figure 32.

![Real Time Email Alert from AMP](https://example.com/image.png)

**Figure 32** Real Time Email Alert from AMP

The table below breaks down the information that the administrator receives as part of the alert.

<table>
<thead>
<tr>
<th>Value</th>
<th>Information on the alert</th>
</tr>
</thead>
<tbody>
<tr>
<td>What is the matching condition for the trigger?</td>
<td>Interference, Channel Utilization</td>
</tr>
<tr>
<td>What is the severity level of the trigger?</td>
<td>Critical</td>
</tr>
<tr>
<td>What are the affected devices?</td>
<td>135-1 and 135-3</td>
</tr>
<tr>
<td>What is the affected radio?</td>
<td>802.11bgn radio on both the APs</td>
</tr>
<tr>
<td>Where are they located?</td>
<td>Location information floor plan level visualization</td>
</tr>
<tr>
<td>Link to More detailed info</td>
<td>Link to the AP monitoring page on AMP that offers detailed statistics</td>
</tr>
</tbody>
</table>

Select the hyperlink provided for AP-135-1 on the alert. The AP monitoring page on AMP opens up.
Select the 802.11bgn radio from AP-135-1’s monitoring page, as shown in Figure 33.
This opens the 802.11bgn radio statistics page. As seen in Figure 34, the issue reported is a high noise floor condition. The reason for the high noise floor condition is the presence of a wideband device fixed frequency interferer. The noise floor and the channel utilization graphs reinforce that this is the issue.

![Figure 34](image)

**Figure 34  Using the Radio Statistics Page for Real-time Troubleshooting**

The interfering device table in the radio statistics page gives interferer-specific information that enables the administrator to determine the duty cycle of the noise source and the channels affected. This allows the administrator to determine whether this is a persistent or a transient noise source with the first/last-seen time stamps as shown in Figure 35.

![Figure 35](image)

**Figure 35  Interference Device Detected**

The vital piece of information required for real-time troubleshooting is the interferer’s location. The visual RF module contains floor plans of the current deployment (imported into AMP by the administrator), the location of the APs and the clients. It also integrates location information for interferers.
The three APs in the network are able to hear the video bridge at different signal levels. With the received signal strength triangulation, the location of the interferer can be approximated on a floor plan.

The AP monitoring page on AMP has a link to the visual RF module as shown in Figure 36. Select the map to maximize it.

This opens the floor plan on the Visual RF module with the location of the three APs and the clients associated. The video bridge in the 2.4 GHz band has been identified and located on the floor plan as
shown in **Figure 37**.

![Interferer location Tracking on AMP](image)

**Figure 37**  Interferer location Tracking on AMP

The spectrum analysis dashboard could be triggered right from the AP monitoring page on AMP to visualize the impact of interference in the form of FFTs and spectrograms as shown in the **Figure 38**.

![Spectrum Analysis Launched from AirWave](image)

**Figure 38**  Spectrum Analysis Launched from AirWave
Managing and Optimizing RF Spectrum for Aruba WLANs

The screenshot below has 4 different charts for visualization namely real-time FFT, FFT duty cycle, swept spectrogram and active devices. From the description of each chart mentioned in the previous section it is evident that Channel 11 is being bombarded with a high energy and a high duty cycle source of interference as shown in Figure 39.

![Spectrum Analysis for the affected AP (AP-135-1)](image)

Aruba WLAN has provided with real-time alerts, RF statistics, interference device detection, classification, location and spectrum visualization. A WLAN administrator now has a sufficient amount of information required to walk down to the area where the device was located and turn it off, thereby restoring reliable RF conditions for the office.

Proactive Troubleshooting with AirWave

AMP has both built-in and custom RF health reports that provide visibility into problem devices, the problem history, and the reason for the occurrence of the problem. This gives the administrators a chance to plan proactively before the users start complaining about RF related issues. In the previous section we have seen how Aruba provides different tools to perform real-time troubleshooting of RF related issues.

In this section we will look at how features such as RF health reports help an administrator to proactively identify RF related issues and resolve them before the user files a trouble ticket. For this use case, we have a pre-generated RF health report for a building that has an Aruba WLAN network. Below we will look at a few examples to see how the information on this report can be used to proactively troubleshoot potential issues.
Example 1: Too Many Channel/Power Changes

Figure 40 lists the problem 2.4 GHz radios on the network. Why does AMP think these are problem devices? Let us pick on AP 12c. From the report you will notice that the channel and power changes on this AP appear to be very high. There has been 92 channel changes and 86 power changes.

<table>
<thead>
<tr>
<th>Device</th>
<th>Channel Changes</th>
<th>Transmit Power Changes</th>
<th>Mode Changes</th>
<th>Average Noise (dBm)</th>
<th>Average Channel Busy (%)</th>
<th>MAC Phy Errors</th>
<th>Interfering Devices</th>
<th>Number of Users</th>
<th>Radio</th>
</tr>
</thead>
<tbody>
<tr>
<td>12c</td>
<td>92</td>
<td>86</td>
<td>0</td>
<td>-96.00</td>
<td>35.47</td>
<td>28153</td>
<td>Cordless Base Freq Hopper (2)</td>
<td>0</td>
<td>0.00</td>
</tr>
<tr>
<td>20c</td>
<td>29</td>
<td>50</td>
<td>0</td>
<td>-96.00</td>
<td>59.69</td>
<td>28191</td>
<td>Cordless Base Freq Hopper (2), Microwave, Video Device Fixed Freq</td>
<td>0</td>
<td>0.00</td>
</tr>
<tr>
<td>02c</td>
<td>2</td>
<td>51</td>
<td>0</td>
<td>-96.00</td>
<td>56.79</td>
<td>101064</td>
<td>Cordless Base Freq Hopper (2), Microwave</td>
<td>0</td>
<td>12.00</td>
</tr>
</tbody>
</table>

Selecting device 12C provides detailed RF related information available on the radio statistics page that we are familiar with. One important piece of information provided on this page is the ARM events history. This table in Figure 41 gives a snapshot of the ARM channel and transmits power changes over a period of time. There has either been a transmit power or a channel change every 5 minutes, and the change reason is given as “interference”.

The radio statistics page also lists out the detected interfering devices. In this particular scenario there are multiple sources of interference such as a microwave oven, video bridge, Xbox, and others. These are devices with different duty cycles that are generating so much energy on the operating channel that is causing ARM to change channel/power more frequently than it is supposed to. From Figure 42 note that the interference sources are present from channel 1 to channel 14 in the 2.4 GHz band, leaving no choice for ARM to pick a cleaner channel.

Detected Interfering Devices

Figure 40       Problem 2.4 GHz

Figure 41       Using the ARM Events Table to Troubleshoot Issues

Figure 42       Using the Detected Interference Devices Table to obtain Details on the Interferers.
This is a scenario where an administrator's manual intervention is required. The administrator has to walk down to the location where this AP is mounted and remove those interference sources from the network. Thus, the RF health report has provided the visibility into the air quality for this particular AP and has enabled the administrator to take proactive measures to improve user experience in the RF neighborhood.

**Example 2: High Channel Utilization on an Access Point**

Let us focus on another parameter shared by the health report. As seen in Figure 43 the table lists the most utilized 2.4 GHz radios in the network. Let us pick on device 52C. Looking at the data that AMP has provided, it is evident that it has a high channel utilization of approximately 72%.

<table>
<thead>
<tr>
<th>Rank</th>
<th>Device</th>
<th>Channel Busy (%)</th>
<th>Interference (%)</th>
<th>Number of Users</th>
<th>Bandwidth (Mbps)</th>
<th>Location</th>
<th>Last Access</th>
<th>Folder</th>
<th>Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>52C</td>
<td>72.44</td>
<td>6.69</td>
<td>0</td>
<td>0.00</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>3</td>
<td>A63</td>
<td>55.91</td>
<td>2.36</td>
<td>0</td>
<td>0.00</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>4</td>
<td>72C</td>
<td>57.76</td>
<td>2.76</td>
<td>0</td>
<td>0.00</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>6</td>
<td>22C</td>
<td>51.57</td>
<td>2.15</td>
<td>0</td>
<td>0.00</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>7</td>
<td>62C</td>
<td>46.95</td>
<td>1.97</td>
<td>0</td>
<td>12.00</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>8</td>
<td>A53</td>
<td>43.70</td>
<td>1.97</td>
<td>0</td>
<td>0.00</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>9</td>
<td>A1</td>
<td>41.73</td>
<td>1.57</td>
<td>0</td>
<td>0.00</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>10</td>
<td>11C</td>
<td>41.73</td>
<td>1.36</td>
<td>0</td>
<td>0.00</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>11</td>
<td>19C</td>
<td>41.16</td>
<td>1.07</td>
<td>0</td>
<td>0.00</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>12</td>
<td>78C</td>
<td>38.58</td>
<td>1.57</td>
<td>0</td>
<td>0.00</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>13</td>
<td>A63</td>
<td>37.61</td>
<td>1.57</td>
<td>0</td>
<td>0.00</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>14</td>
<td>18C</td>
<td>35.43</td>
<td>1.97</td>
<td>0</td>
<td>0.00</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>15</td>
<td>A13</td>
<td>33.46</td>
<td>1.97</td>
<td>0</td>
<td>0.00</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

**Figure 43**  **Most utilized Radios as per the RF Health report**

Drilling down into device 52C the radio statistics page shows the real-time channel utilization graph for the last 3 months. As seen in Figure 44 It has consistently been greater than 70%.

**Figure 44**  **Channel Utilization Graph on the Radio Statistics Page of AMP**

This is an indication to the WLAN administrator that the AP has been over-utilized for a long period of time. There are some demanding users in the area who have been utilizing more than half of the available bandwidth. This could be a measure that indicates the RF neighborhood requires more APs to support the demands and higher capacity of the users and applications. This is a critical tool for network administrators for capacity planning and performance issue avoidance.
Conclusion

Aruba WLAN provides a window into the RF environment that provides visibility into interference sources and the problems that can result in performance degradation. Without an integrated spectrum analysis solution it is virtually impossible for administrators of these systems to isolate interference in sites with high client densities, latency sensitive multimedia applications or electromagnetically challenging RF environments. It is the foundation for a wide range of services that enhances enterprise WLAN performance and functionality. Combined with ARM technology, the spectrum analyzer fully automates interference detection, classification and mitigation without requiring manual intervention or additional hardware. Bringing AMP into the architecture introduces critical features like real-time troubleshooting, location tracking of interference sources, health reports for proactive troubleshooting and history into ARM events. The WLAN administrator now has visibility into the RF environment, and leveraging an integrated spectrum analysis and network management solution has the capacity to resolve problems without requiring an RF PhD.
Appendix A: Contacting Aruba Networks

Contacting Aruba Networks

<table>
<thead>
<tr>
<th>Web Site Support</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Main Site</td>
<td><a href="http://www.arubanetworks.com">http://www.arubanetworks.com</a></td>
</tr>
<tr>
<td>Support Site</td>
<td><a href="https://support.arubanetworks.com">https://support.arubanetworks.com</a></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Support Emails</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Americas and APAC</td>
<td><a href="mailto:support@arubanetworks.com">support@arubanetworks.com</a></td>
</tr>
<tr>
<td>EMEA</td>
<td><a href="mailto:emea_support@arubanetworks.com">emea_support@arubanetworks.com</a></td>
</tr>
<tr>
<td>WSIRT Email Please email details of any security problem found in an Aruba product.</td>
<td><a href="mailto:wsirt@arubanetworks.com">wsirt@arubanetworks.com</a></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Validated Reference Design Contact and User Forum</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>VRD Contact Email</td>
<td><a href="mailto:referencedesign@arubanetworks.com">referencedesign@arubanetworks.com</a></td>
</tr>
<tr>
<td>AirHeads Online User Forum</td>
<td><a href="http://community.arubanetworks.com">http://community.arubanetworks.com</a></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Telephone Support</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Aruba Corporate</td>
<td>+1 (408) 227-4500</td>
</tr>
<tr>
<td>FAX</td>
<td>+1 (408) 227-4550</td>
</tr>
<tr>
<td>Support</td>
<td></td>
</tr>
<tr>
<td>United States</td>
<td>+1-800-WI-FI-LAN (800-943-4526)</td>
</tr>
<tr>
<td>Universal Free Phone Service Numbers (UIFN):</td>
<td></td>
</tr>
<tr>
<td>Australia</td>
<td>Reach: 1300 4 ARUBA (27822)</td>
</tr>
<tr>
<td>United States</td>
<td>1 800 9434526 1 650 3856589</td>
</tr>
<tr>
<td>Canada</td>
<td>1 800 9434526 1 650 3856589</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>BT: 0 825 494 34526 MCL: 0 825 494 34526</td>
</tr>
</tbody>
</table>
## Telephone Support

- **Universal Free Phone Service Numbers (UIFN):**

  - **Japan**
    - IDC: 10 810 494 34526 * Select fixed phones
    - IDC: 0061 010 812 494 34526 * Any fixed, mobile & payphone
    - KDD: 10 813 494 34526 * Select fixed phones
    - JT: 10 815 494 34526 * Select fixed phones
    - JT: 0041 010 816 494 34526 * Any fixed, mobile & payphone

  - **Korea**
    - DACOM: 2 819 494 34526
    - KT: 1 820 494 34526
    - ONSE: 8 821 494 34526

  - **Singapore**
    - Singapore Telecom: 1 822 494 34526

  - **Taiwan (U)**
    - CHT-I: 0 824 494 34526

  - **Belgium**
    - Belgacom: 0 827 494 34526

  - **Israel**
    - Bezeq: 14 807 494 34526
    - Barack ITC: 13 808 494 34526

  - **Ireland**
    - EIRCOM: 0 806 494 34526

  - **Hong Kong**
    - HKTI: 1 805 494 34526

  - **Germany**
    - Deutsche Telkom: 0 804 494 34526

  - **France**
    - France Telecom: 0 803 494 34526

  - **China (P)**
    - China Telecom South: 0 801 494 34526
    - China Netcom Group: 0 802 494 34526

  - **Saudi Arabia**
    - 800 8445708

  - **UAE**
    - 800 04416077

  - **Egypt**
    - 2510-0200 8885177267 * within Cairo
    - 02-2510-0200 8885177267 * outside Cairo

  - **India**
    - 91 044 66768150