Competitive Test Report

October 2016

Mojo Networks C-130 vs. Aerohive AP250, Aruba AP-335,
Cisco 3800, Meraki MR53, and Ruckus R710

Introduction

In September 2016, Mojo Networks conducted an "Access Point Performance with WIPS" benchmark test to evaluate both the impact of WIPS monitoring on dual-band, mixed application performance and the timeliness and effectiveness of rogue access point detection and prevention.

The Results

The results of the performance impact testing showed that dual radio access points with background scanning enabled impact the client user experience negatively, while access points that leverage a third radio to perform scanning functions did not impact the client experience negatively.

The second part of the test intended to show the results of each access point's WIPS functionality in terms of how quickly and accurately each solution detected and reacted to a rogue access point, however in the end there were no times to compare because only the Mojo C-130 was able to detect, classify, and prevent the rogue access point used for this test.

Table 1

AP Make	Mojo	Aerohive	Meraki	Cisco	Ruckus	Aruba
Model Tested	**C-130**	**AP250**	**MR53**	**3802i**	**R710**	**AP-335**
WiFi Chipset	QCA9994	BCM43525	--*	Marvell 88W8964	QCA9990	QCA9994
802.11 Version	11ac W2	11ac W2	11ac W2	11ac W2	11ac W2	11ac W2
MIMO Streams	4x4:4	3x3:3	4x4:3	4x4:3	4x4:4	4x4:4
2.4GHz (Mbps) Max Throughput	800	600	800	2600**	800	800
5GHz (Mbps) Max Throughput	1733	1300	1733	2600	1733	1733
SW Version Tested	8.1.1.81	7.0r2 Build 131568	9/13/2016	8.3.102.0	9.12.1.0 Build 148	6.5.0.0

* Chipset details not readily available

** Flex radio at 5GHz

Test Configuration

Wireless testing is challenging because there are many variables that are difficult to control, account for, or work around. If something changes during a test or between test runs, it can change the result and the reproducibility of the test.

Mojo strives to produce fair and reproducible results. We know our products are as good or better than the best of the competition and are not afraid of a fair comparison. For each test, we configure each AP system in accordance with the manufacturer's published, recommended best practices, and at the beginning of the test, we upgrade the AP to the most current version of AP code available.

This summary provides an overview of the test results. The details of each individual test including AP system configurations, and test methodology will be shared in detailed test reports.

All tests were conducted in Mojo Network's performance test lab by Senior Technical Marketing Engineer Robert Ferruolo.

Mojo Networks Performance Test Lab

The access points were tuned for performance and rogue detection. The only significant changes made from default were:

- Real-time application deferrals of WIPS scans were disabled. Otherwise the real-time applications would have prevented those access points from performing WIPS scanning.
- Aerohive's scan time was change from the default of 10 minutes to it minimum of 1 minute so it would detect rogues more quickly.

For detailed parameters and configuration settings see Appendix A.

Overview

Enterprise networks typically leverage some form of persistent wireless scanning such that all other available channels (in the 2.4 and 5GHz spectrum) outside of that which is used directly by the access point itself can be monitored. These "off-service channels" are monitored to evaluate their radio characteristics (i.e. channel utilization, quantity of other nearby access points, interference, etc.) and to look for security issues such as rogue access points and rogue clients. Rogue access points and clients are defined as those that are connected to the corporate network but are not authorized to do so.

Dual-radio access points use a technique known as 'background scanning' to monitor off-service channels. In short, they regularly "hop" to these channels for small intervals of time in order to scan for the necessary data they require for functions like WIPS or RRM. More recently, access points have been engineered with three radios; with three radios an access point can dedicate the third radio to channel scanning so as to not split a radio's time between serving clients and scanning. Dividing the radio's attention like this can have two negative effects:

1. Client performance and satisfaction can be reduced
2. Rogue detection and prevention takes much longer, or in some cases fails, depending on the rogue type/configuration

Since one test is used to evaluate two criteria, the results are reported in two sections:

- Access Point Performance – determined the number of clients who were provided the minimum service levels
- Rogue Detection – detection and prevention times and proper classification of rogue vs. neighbors

Access Point Performance

The access point performance part of this test monitored clients on both the 2.4 and 5GHz radios that were using a mixture of data, voice, and video traffic, sourced by IxChariot. The test was run three times for each access point and the best of the three runs was used for evaluation.

Client Configuration

The 2.4GHz radio supported six clients in total (two per application) and the 5GHz radio supported twenty clients in total (ten data, five voice, and five video). See Table 1 for more details.

Table 1

Radio Band	Application Type	Packet Direction	Number of Clients	Client Model	802.11 Capabilities
2.4GHz	Voice	Bi-directional	2	Acer F15	802.11ac 1x1
	Video	Downstream	2		
	Data	Upstream	1		
		Downstream	1		
5GHz	Voice	Bi-directional	5		
	Video	Downstream	5		
	Data	Upstream	5		
		Downstream	5		

Application Service Levels

The results from each test were evaluated against predefined service levels (see Table 2), where the number of clients that met or exceeded the service level relative to their specific application were reported as passing. The following metrics were used to establish the minimum acceptable service level for the clients per application. These services levels are in line with industry standards for access point load tests.

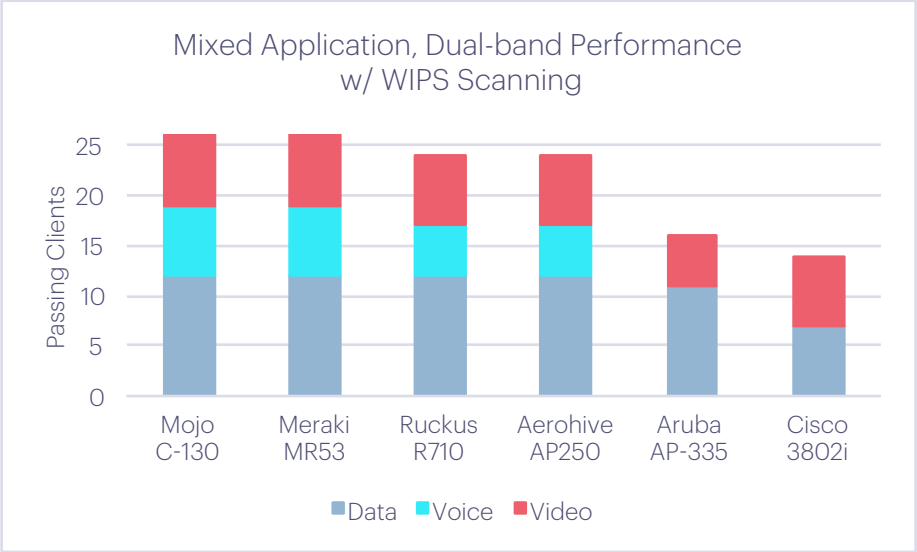
Table 2

Application	Service Level
Data	>= 1 Mbps
Voice	>= 4.2 MOS
Video - Delay Factor	<= 50ms
Video - Media Loss Rate	<= .004

Application Performance Results

The access points with three radios (Mojo C-130 and Meraki MR53) met the SLA for all applications and clients. The Aruba AP-335 and Cisco 3800 suffered greatly, with only 62% and 54%, respectively, of their clients attaining the required level of service to receive a passing grade.

Figure 1



Access points without a third radio suffered because they must time slice their service radios between serving clients to meet an SLA and background scanning to find rogues. Background scanning impacts any application that requires network packets to be delivered in a timely, uninterrupted fashion. In particular, if voice or video packets are delayed, they will ultimately arrive too late for the application to use them and are thrown away as a result. The two charts below clearly show the impact of background scanning on voice quality (i.e. MOS or Mean Opinion Score) during this test.

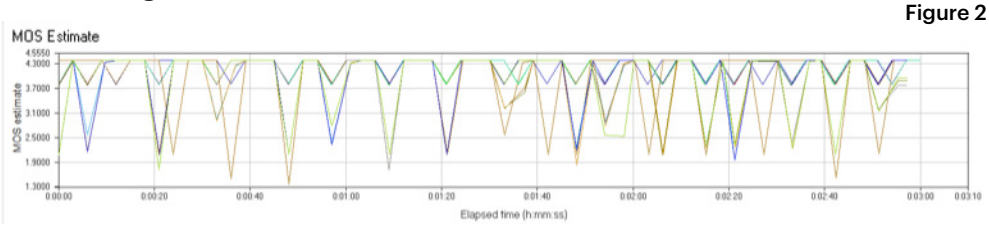
MOS During Background Scanning

The following chart shows what happens to voice traffic when the radio delivering the audio frames goes off its native channel to perform off-service channel scans for WIPS or RRM functions. In this case the radio goes off channel every 10 seconds to perform a scan that lasts for approximately 100 milliseconds. When this occurs the MOS dips significantly, indicating a negative impact on the user experience.

Voice MOS Estimates - Background Scanning

Figure 2

When the access point goes off-channel, it queues packets until its return to the native channel. Queuing packets is especially challenging for real-time applications that need to receive packets at regular, predictable intervals.

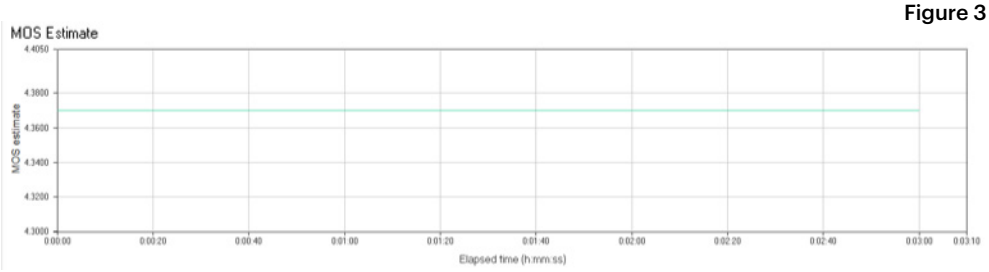


When the access point returns to its native channel, it catches up by delivering all the queued packets to the client as quickly as it can. The process of bunching packets together and bursting them out all at once can overwhelm the real-time application's jitter buffer, causing pixelation, freezing or skipping in the audio or video stream, and negatively impacting the user experience.

MOS Using the C-130 (Tri-Radio Access Point)

Since the C-130 uses a third radio for off-service scanning there is no impact to the voice quality. The chart below shows a test run with seven voice clients connected to a C-130. The flat line at a MOS of 4.37 represents all seven voice clients; since there was no variation in the individual graph lines only one can be seen. The other six lines are masked by the last line plotted (light blue).

Figure 3



Note that a MOS of 4.37 is the best score that is achievable in this given scenario. MOS is affected by many attributes included the CODEC used, network latency, packet jitter, and packet loss.

WIPS Performance

The second component of this test evaluated the access point's ability to detect, categorize, and prevent a rogue access point and its clients. This test was performed by connecting an Apple Airport Express access point via Ethernet on the same subnet as the access point under test. The rogue Airport Express broadcast its rogue SSID on both the 2.4 and 5GHz bands and a rogue client was connected to each band.

The evaluation success criteria looked at two primary objectives.

1. How long did it take the access point undergoing the test to detect and shut down the rogue access point and its associated clients
2. How successful was the access point in differentiating the rogue access point from non-threatening neighboring access points.

Rogue Access Point / Configuration (see Appendix C for more details)

- Apple Airport Express (802.11n)
- SSID on 2.4 and 5GHz
- No encryption
- NAT enabled

Table 3

Access Point Make/Model	Detection	Prevention	Identification	
			Rogue	Neighbor
Mojo C-130	Yes	Yes	Rogue	Neighbor
Aerohive AP250	No	No	Neighbor	Neighbor
Aruba AP-335	No	No	Suspected Rogue	Suspected Rogue
Cisco 3800	No	No	Rogue / Unclassified Rogue	Rogue / Unclassified Rogue
Meraki MR53	No	No	Other SSID	Other SSID
Ruckus R710	No	No	Active Rogue	Active Rogue

Conclusion

Access Point Performance Conclusion

From this test we can infer that background scanning negatively impacts the user experience since none of the two radio access points managed to attain the minimal service level for every client. Only three radio access points met the minimum service level for all clients and applications.

Background scans impact real-time packet delivery by increasing jitter and bursting queued packets. The degree of impact to the user experience depends on how well each voice or video application handles packet jitter and "bunchiness".

Rogue Detection Conclusion

All access points except for the Mojo C-130 failed the first success criterion, as they were unable to either detect or prevent the rogue access point and its clients.

For the second success criterion, all access points except the Mojo C-130 miss-identified either the rogue or the neighboring access points. They were unable to differentiate between the two, and in every case classified both the rogue access point and neighboring access point as either "Rogue" or "Neighbor". Since there is no common verbiage between access point vendors please review Table 3 for the specific classifications.

Classifying everything as one type is dangerous and undermines the effectiveness of wireless security measures. On the one hand, when rogue and neighboring access points are all classified as "Rogue", it becomes impossible to validate them all, and "rogue fatigue" sets in leading to ignored results. On the other hand, if they are both classified as "neighbor" or "external" (or something else equally benign), a false sense of security kicks in and organizations are unaware of the actual threats on the network.

Why should you believe us? Because we have nothing to hide. We know our solution is as good or better than our competitors and feel confident in the reproducibility of our results.

As a result, we encourage you to validate our results. For each test mentioned in this report we will provide a comprehensive report that will include the test results, the test methodology, and the tested access point system configurations: all the information needed to reproduce our results.

We will also meet any AP manufacturer in a head-to-head performance test, with the following rules:

- Testing is apples-to-apples
- Hardware, firmware, and software under test is at the latest version and generally available
- Testing will be overseen by a mutually-agreed-upon, independent WiFi industry leader, who will:
  - Act as an arbiter
  - Confirm the test bed, environment, and methodology
  - Validate WLAN configurations, optimizations, hardware, and versions of code
  - Publish the results

If you have questions about these tests, or anything else related to Mojo Networks, please feel free to reach us at

info@mojonetworks.com or call us at +1 (877) 930-6394.

Appendix A

Environment	Setting	Notes
Cabled or Over-the-Air	Over-the-Air	
AP-to-Client Distance	3 - 15 feet	
Performance Parameters	**Setting**	**Notes**
Power	POE+	All fully powered
Bands tested	2.4 and 5GHz	Clients on both bands concurrently
Channel	Same	All access points were tested using the same channels after verified clean
Channel Width	2.4/20, 5/80	
AP Mode	Bridged	
A-MPDU	Enabled	
A-MSDU	Enabled	
MU-MIMO	Enabled	
Short Guard Interval	Enabled	
MCS Rates	0-9	
Tx Power	Max	
Security	PSK/AES	
Rate Limiting	Default	
QoS Rules	Default	
WMM	Enabled	
App Visibility and Control	Disabled	
Scanning Parameters	**Setting**	**Notes**
Background Scanning	Enabled	N/A for C-130 and MR53 due to 3rd radio
WIPS	Enabled	
WIPS Channels Scanned	All	
WIPS Scan Interval	Default*	Aruba: 10 seconds Aerohive: 1 minute (changed from 10 minutes) Cisco: 16 seconds Ruckus: 20 seconds
Spectrum Monitoring	Disabled	
Voice Aware	Disabled	
Video Aware	Disabled	
Power Save Client Aware	Disabled	
Channels Scanned	All	

Appendix B – Test Procedure

1. Enable background scanning on all 2-radio access points
2. Configure the 2.4GHz band to channel 6/20MHz and configure the 5GHz band to channel 149/80MHz
3. Enable access on both bands
4. Associate 6 Acer F15 clients to the 2.4GHz band and 20 Acer F15 clients to the 5GHz band
5. Configure an Apple AirPort as an Open/NAT access point
6. Connect the Apple AirPort via Ethernet to the same network as the access point under test (APUT)
7. Power on the Apple AirPort and start the IxChariot test (3 minutes)
8. Monitor the air to see when the AirPort starts broadcasting its SSID (using InSSIDr or NetSpot)
9. Start timer as soon as the AirPort SSID is seen
10. Associate a client to rogue access point's 2.4 GHz channel and another client to the 5GHz channel and browse the Internet
11. Record the time that the AirPort is detected as a rogue
12. Record the time that rogue is prevented by testing network connectivity of rogue clients on both bands

Appendix C – Rogue Equipment

Rogue Access Point	Model	802.11 Capabilities	Band	Settings
1	AirPort Express	802.11n	2.4 and 5GHz	• Open • NAT • Non MAC Adjacent

Rogue Clients	Model	802.11 Capabilities	Band
1	iMac	802.11ac Wave 1 3x3	2.4GHz
1	OnePlus 2	802.11ac Wave 2 1x1	5GHz

The Global Leader in Secure Wi-Fi Solutions
Mojo Networks, Inc. 339 N. Bernardo Avenue #200, Mountain View, CA 94043
T +1.877.424.7844 T 650.961.1111 F 650.961.1169 **www.mojonetworks.com** **info@mojonetworks.com**

mojo Networks