A Comparison of Efficiency, Throughput, and Energy Requirements of Wireless Access Points

March 2009

Anthony Murabito
University of New Hampshire
InterOperability Laboratory
WLAN Consortium

A Comparison of Efficiency, Throughput, and Energy Requirements of Wireless Access Points

Executive Summary

As energy sources are dwindling, power consumption is a major obstacle facing virtually every industry. Alongside Internet access, wireless computer networks, more commonly known as Wi-Fi networks, have become widely adopted.

These wireless networks have found their way into our homes and have also spread to the enterprise market. Typical deployment of a Wi-Fi network consists of one or more wireless Access Points serving multiple end-user stations such as laptops, PDAs, and recently even cell phones.

The goal of this research is to study the power consumption of wireless Access Points, and determine possible means to reduce the energy requirement of the Access Point. In the first phase of this research, we will test a range of Access Points made available to us as through a partnership with the University of New Hampshire InterOperability Laboratory (UNH-IOL).[1]

The second phase of the project will be dedicated to studying the impacts of modifying various configuration parameters. To accurately compare the amount of electrical energy consumed by a wireless Access Point we will be using a P3 International P4400 KILL-A-WATT™ wattmeter.[2] In the conclusion, we hope to provide guidelines for purchasing and operating Access Points from the perspective of energy consumption.

Examining Access Point Power Consumption

The basic purpose of a wireless Access Point is to provide an entry point for wireless devices onto a wired network. Wireless Access Points are complex devices with many configurations and settings that can be modified. Changing these values can result in higher load on a device and may increase power consumption of some of the Access Point's electrical components. We will be exploring throughput, efficiency, and energy requirements of three leading vendors who produce Wireless Access Points: AP1, AP2, and AP3. Exact make and models have been excluded to promote a fully objective and non-biased viewpoint. All of these Access Points support IEEE 802.11a, IEEE 802.11b, and IEEE 802.11g operational modes.

Influential Factors Affecting Power Consumption

1.**Hardware Platform and Electrical Components** – All of the components embedded onto a circuit board consume power, or modify power. Different wireless chipsets, hard-wired chipsets, IEEE 802.11 radios, and power amplifiers, all have the ability to modify the amount of power an Access Point may consume. In addition to factors such as transmit power, the rate at which digital information is transmitted can play a large factor in power consumption. When comparing IEEE 802.11b and IEEE 802.11g wireless network traffic, IEEE 802.11b traffic requires more power. This is because the data rates which IEEE 802.11b uses to transmit are at a much slower speed, so it takes a greater amount of time to transmit the same amount of data as it would at a higher rate. As technologies improve, often times manufacturers will produce new hardware revisions which may showcase new features, as well as change the energy requirements of an Access Point.

2.**Hardware Interoperability** – When selecting different components to build an Access Point, it is important to consider how well they operate together in an electrical sense. Some components may work together flawlessly, while others may require additional resistors, or capacitors in order for the devices to properly operate together. Aside from power used by the wireless radio itself, it is important to consider all of the inner components and how they work together while consuming power.

3.**Software Design –** The software data structures, protocols, and methods used in a wireless network implementation can have a large impact on how quick and effective data processing can be. Some software algorithms can accomplish the same task, but can be orders of magnitude faster, and much more efficient than others. Less efficient code can cause a higher resource demand, and therefore increase the energy requirements of an Access Point.

Test Methodology

As concern regarding energy sources continues to rise, it is important to attempt to find solutions to reduce the power consumption of common products. Wireless Access Points have become increasingly popular; according to a study done by research firm Parks Associates, 52% of U.S. households with a computer network use wireless technology.[3] This clearly shows that wireless network use is becoming more widely adopted than wired networks in the home. The popularity of wireless networks in the enterprise market has also increased over the years as corporations embrace the ease of installation and convenience of wireless networks.

Growing demand and deployments of wireless translates to an increased power requirement; each Access Point will need to be powered in some fashion or another. A seemingly small difference of a few watts could easily correspond to a few hundred watts when considering a large deployment; it is important to take into consideration the actual power consumption of every individual unit.

To accurately record the power consumed by each Access Point, we plug each unit into a P3 International P4400 KILL-A-WATT™ electricity usage monitor and record the changes in power draw from the Access Points tested under different conditions.

Typically, the radio front end of a wireless Access Point is designed using a Class A power amplifier to increase the radiated signal strength leaving the antennae to levels suitable for over-the-air operation. This class A amplifier requires the Access Point to have a fairly constant power draw, but often causes the AP to waste power on a regular basis. Conversely, this prevents power fluctuations from actually occurring when the Access Point may need less power than it is supplied.

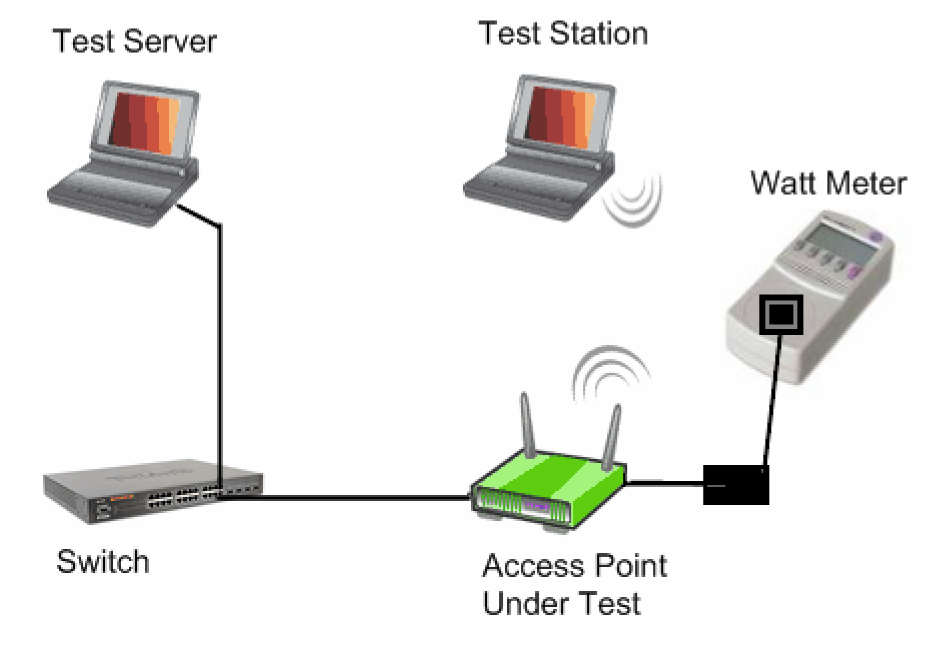
However, this Class A circuit is often part of a tiered power generation system that can be increased by activating other parts of the circuit board, such as additional IEEE 802.11 radios, or additional processors to help distribute load.

Test Setup

A Wi-Fi certified 802.11a/b/g Station was selected to use as a benchmark for testing the different types of Access Points. This test station was installed on a Dell Inspiron 1150 with Windows XP PRO SP2 2002. System specs include: Intel Celeron @ 2.4GHz, 512 MB RAM. This wireless station was configured using Juniper/Funk Odyssey Wireless Configuration Utility.

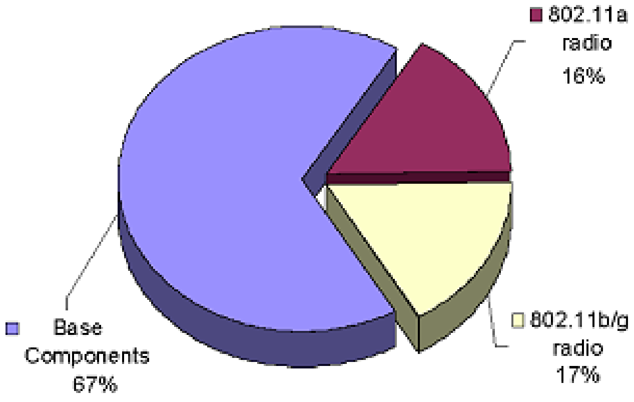
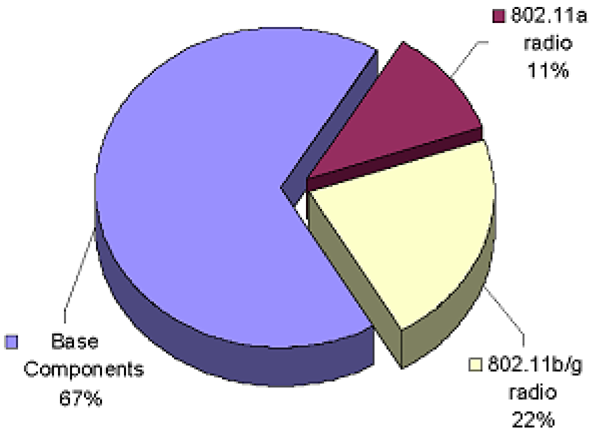
In many tests, a server was required to generate traffic to be forwarded through the Access Point under test. The server used was a Dell Latitude D830 with Windows XP PRO SP2 2002. System specs include: Intel Core 2 DUO T7100 @ 1.80 GHz, 1GB RAM, w/ Broadcom netXtreme 57xx Gigabit Ethernet Controller. See Figure 4 for a graphical interpretation of the test setup.

Figure 1 - Network Test Setup



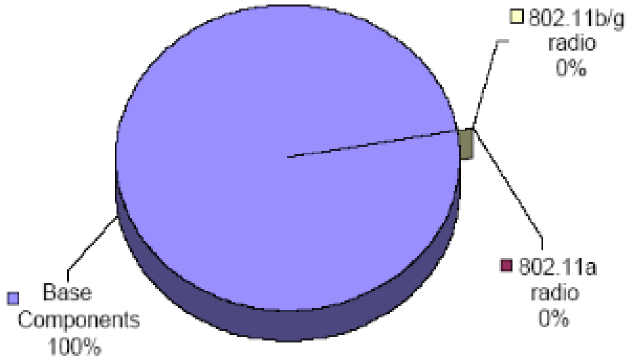
The Test Server ran IXIA IxChariot to generate traffic for throughput, and also collected latency timings. These tests were performed multiple times to ensure accuracy and repeatability. This testing was performed on a private network, within an RF/EMI isolated environment. The following graphs depict the Access Points used in the test setup, and their respective tiers of power consumption.

All of the selected Access Points supported 802.11a/b/g operational modes, and are considered to be enterprise grade Access Points. AP1 utilized four separate antennae, two of which were for 5 GHz operation, and two for 2.4GHz operation. AP2 utilized two antennae for both 2.4 and 5 GHz operation. AP3 had a similar physical layout to AP2, with only two antennae for both 2.4 and 5 GHz operation.

AP1 Power Consumption *Figure 2 AP1 Power Breakdown @ 9 Watts Total*  	AP1 consumed the most power out of the three enterprise-grade Access Points, with a total draw of 9 watts when both of the internal radios were enabled. With both 802.11 radios disabled, AP1 consumed power at a rate of 6 watts. With the 802.11a radio enabled the AP consumed power at a rate of 7 watts, on the other hand having just the 802.11b/g radio enabled the AP consumed power at a rate of 8 watts.
AP2 Power Consumption *Figure 3 AP2 Power Breakdown @ 6 Watts Total*  	AP2 consumed the least amount of power out of the three enterprise grade Access Points, with a total draw of 6 watts when both of the internal radios were enabled. The base components consumed electrical energy at a rate of 4 watts, and each 802.11 radio (a, b/g) consumed about a watt each when turned on.

AP3 Power Consumption

Figure 4 – AP3 Power Breakdown @ 6 Watts Total



AP3 is a prime example of a Class A circuit that has no tiered system of power consumption, and consistently draws the same amount of power regardless of enabled radios. This AP would consistently draw 6 watts of power whether the internal 802.11 radio was set to transmit 11a or 11b/g.

Examining Enterprise Access Point Throughput Results

Throughput is a measure of how much data can be pushed through a network node, and in our case, through a wireless Access Point. Latency can be understood as the delay that occurs between a sender's transmission, and a receiver's reception of a data packet, and is usually measured in milliseconds (ms). The two concepts are inextricably linked, and often a topic of interest when considering network performance. Detailed test results showing throughput values and latency timings can be found in Appendix A, and the summarized results can be found below in Figure 5 and Figure 6.

The Open configuration represents no form of encryption/security employed for the Wireless Local Area Network (WLAN). WPA-TKIP refers to Wi-Fi Protected Access, and is a form of midrange security based on the Temporal Key Integrity Protocol (TKIP), and using an RC4 encryption cipher. WPA2-AES is one of the highest forms of security for a WLAN, and is based on the Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP), using the Advanced Encryption Cipher (AES). All tests were run using 802.11b/g mode using a Pre-Shared-Key(PSK) for any security configuration.

Figure 5 - Comparative TCP Throughput (Mbps)

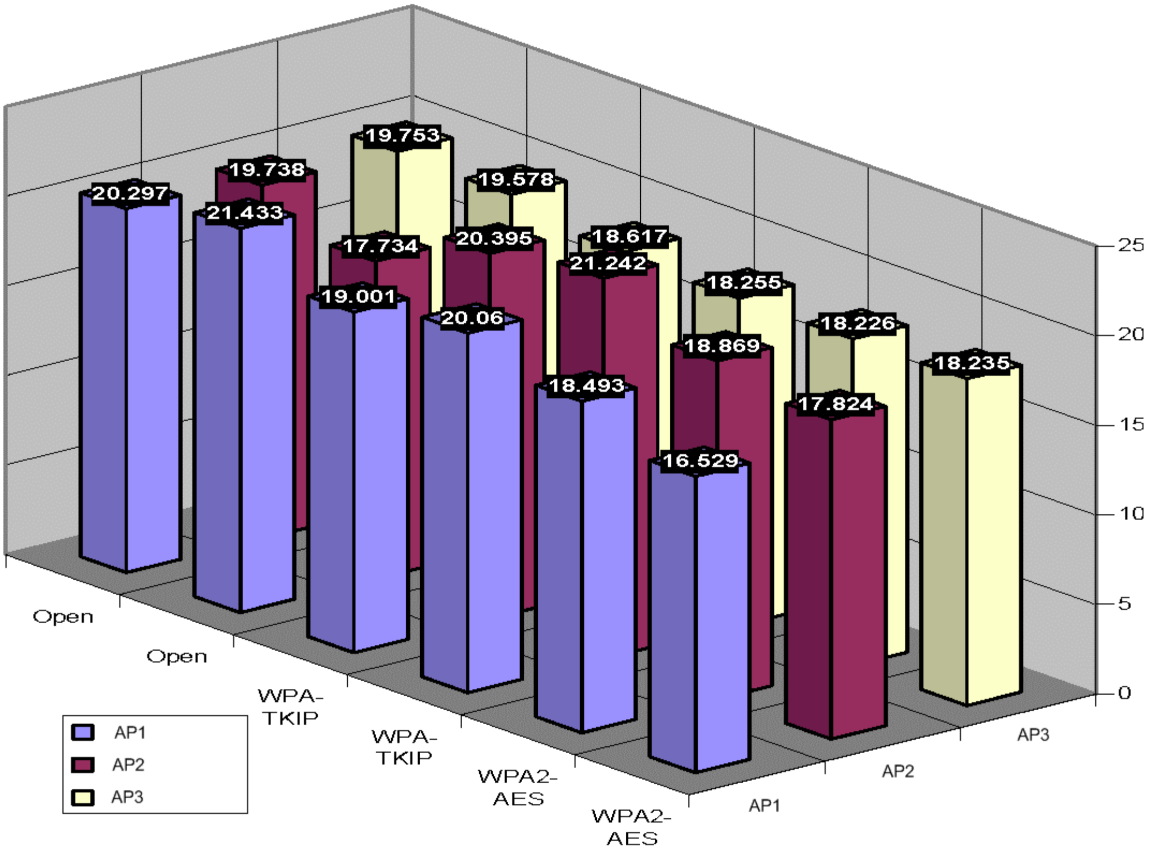


Figure 5 shows the average throughput obtained from running a High Performance Throughput script from IxChariot. These values represent the average TCP throughput of each Access Point in Mega bits per second , where Megabit is the mathematical equivalent of one million bits. Each 60-second test was run twice to ensure accuracy and consistency, and also each test was run with the three different security configurations.

Figure 6 - Comparative UDP Throughput (Mbps)

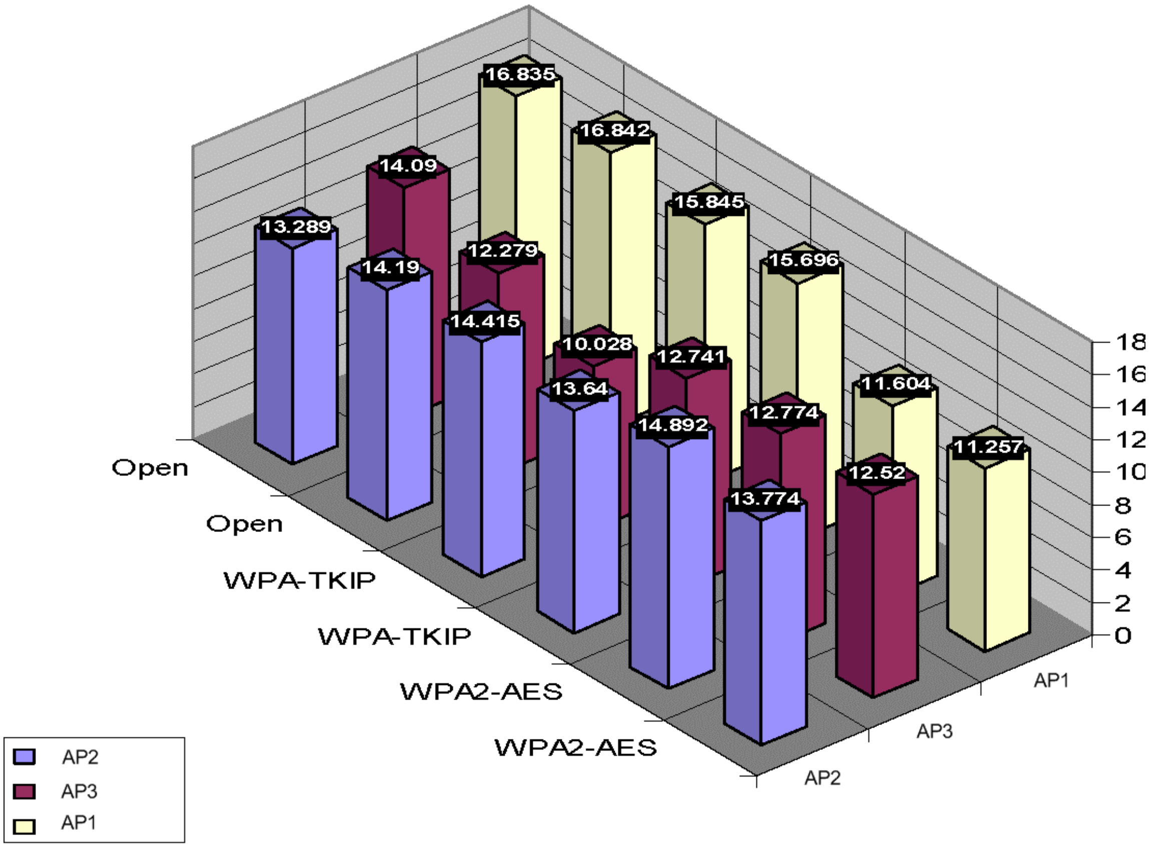


Figure 6 shows the average throughput obtained from running a generic Throughput script from IxChariot. Unfortunately, there was not a High Performance Throughput script available for UDP. These values represent the average UDP throughput in Mbps of each Access Point over a 10 second period, running with three different security configurations. Each of these tests was run twice to ensure accuracy.

Figure 5 and Figure 6 have a common trend: they show that in general, throughput holds an inverse relationship with security. The more security functions applied, the less throughput achieved. This is caused by the extra overhead needed to transmit encrypted frames, which extends the length of MAC layer frames.

Latency values were also recorded, and detailed results can be found within Appendix A. These values were consistent through all tested Access Points, and varied between 1 and 2 milliseconds.

Comparing Throughput and Energy Requirements

Each Access Point consumed a specific amount of electrical energy when running the throughput tests with the 802.11b/g radios enabled. AP1 consumed 8 watts, AP2 5 watts, and AP3 a consistent 6 watts. When we compare these power requirements to the throughput values that each Access Point achieved, we end up with a much better comparison: the amount of electrical energy required to push a significant amount of data through the Access Point. In Figure 7, we can see that for TCP traffic, AP2 is the most efficient model tested. The unit used is Joules per Megabit, where a Megabit is the equivalent of one million bits.

Figure 7 – TCP Efficiency in Joules per Megabit

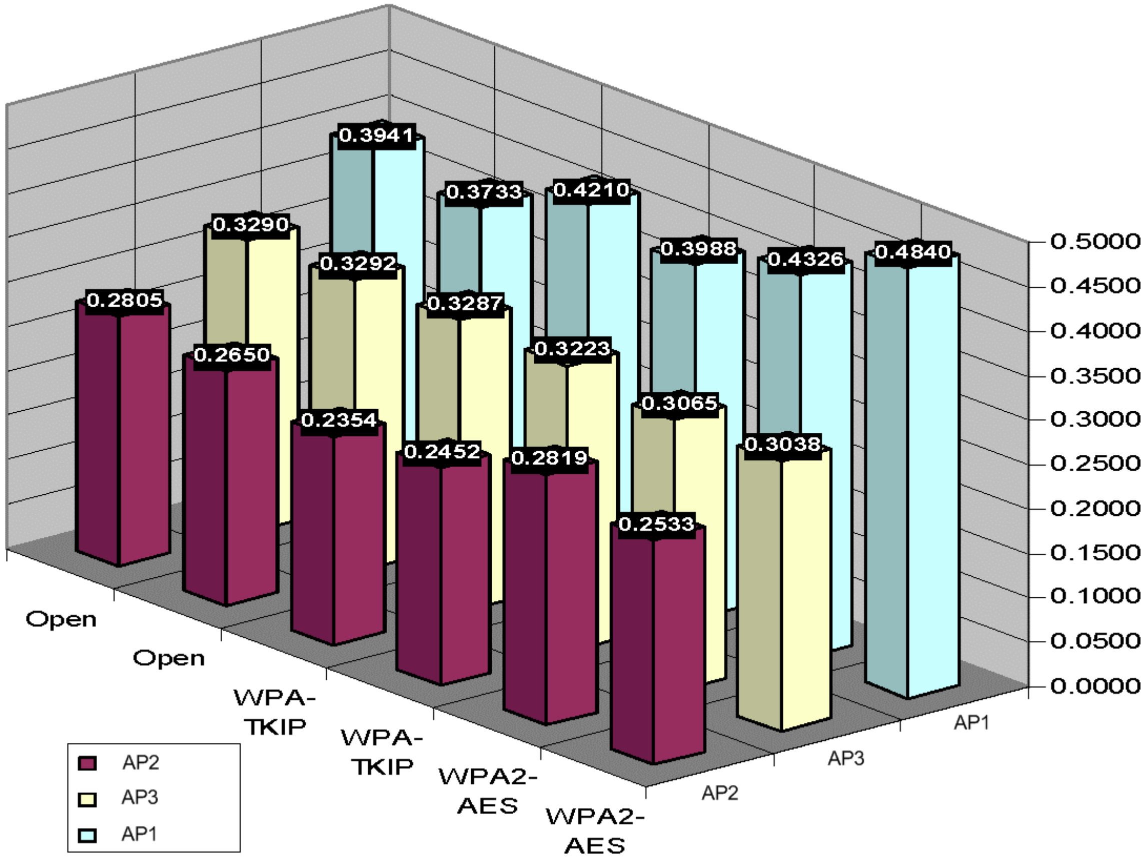
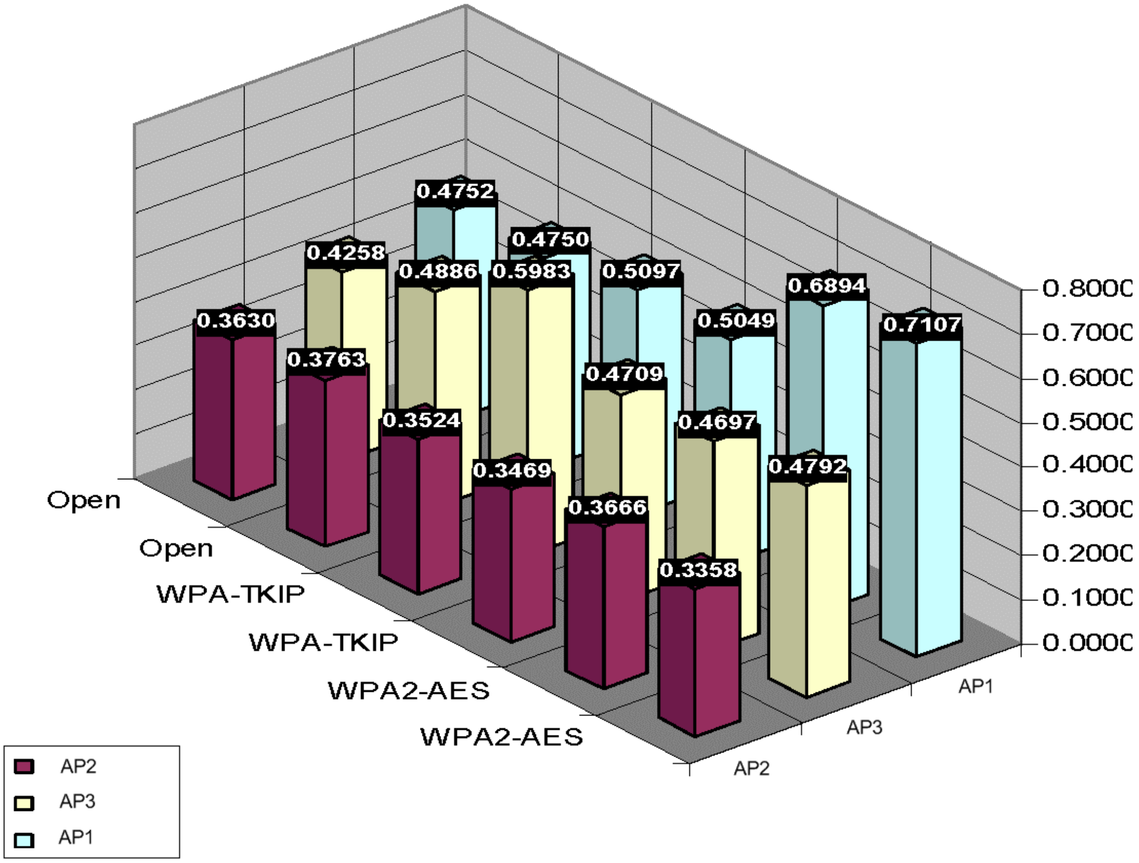


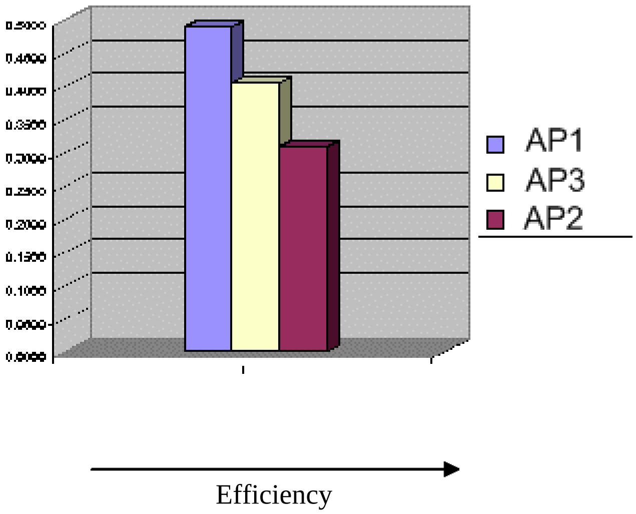
Figure 8 - UDP Efficiency in Joules per Megabit



In Figure 8, we can again see the efficiency of each Access Point, but with UDP as the network protocol. Once again, AP2 ranks as the most power efficient, with the best power to throughput ratio. It is interesting to note, in Figure 8, the drop in efficiency (increase in bar graph size) for AP1 when enabling WPA2-AES encryption. This is most likely caused by powering the extra hardware components necessary to encrypt & decrypt using the AES block cipher. It is also interesting to note that AP2 manages to be twice as efficient when performing a UDP throughput test using WPA2-AES encryption.

Figure 9 illustrates the Average Efficiency in Joules per Megabit of each of the three Access Points tested. The lowest value is desirable in this graph, where AP2 represents the Access Point that was observed to transmit the most amount of information using the least amount of power.

Figure 9 - Comparing Average Efficiency (Joules per Megabit)



Conclusion

Power consumption is a major concern of many industries, and power saving technologies have already been implemented for the station side of wireless networks. As efforts are made to increase the efficiency of everyday electronics, new products come into the scene that conform to more energy efficient standards. There has already been a task force formed by IEEE to study and determine how to mitigate Access Point power consumption.

From the work we have performed here we have found that turning off unused 802.11 radios can significantly decrease the amount of power needed for an Access Point. Also, we can see in Figure 9 that all Access Points do not consume the same amount of power, and under certain conditions such as throughput tests, some Access Points can be over twice as efficient. AP2 averaged the optimal power to throughput ratio, and therefore was the most efficient model tested. These results should be taken into consideration when deploying any large scale 802.11 network, as a significant amount of power can be saved by choosing a more efficient Access Point.

Appendix A: Throughput Test Data

Device	Security	Protocol	Script Name	Throughput	Throughput	Joules Per
				95% CI	Avg.(Mbps)	Megabit
AP1	**Open**	TCP	High_Performance_Throughput.scr	1.258	20.297	0.3941
AP1	**Open**	TCP	High_Performance_Throughput.scr	0.958	21.433	0.3733
AP1	**Open**	UDP	Throughput.scr	0.15	16.835	0.4752
AP1	**Open**	UDP	Throughput.scr	0.146	16.842	0.4750
AP1	**WPA-TKIP**	TCP	High_Performance_Throughput.scr	0.768	19.001	0.4210
AP1	**WPA-TKIP**	TCP	High_Performance_Throughput.scr	2.839	20.06	0.3988
AP1	**WPA-TKIP**	UDP	Throughput.scr	0.123	15.845	0.5049
AP1	**WPA-TKIP**	UDP	Throughput.scr	0.172	15.696	0.5097
AP1	**WPA2-AES**	TCP	High_Performance_Throughput.scr	0.07	18.493	0.4326
AP1	**WPA2-AES**	TCP	High_Performance_Throughput.scr	2.9	16.529	0.4840
AP1	**WPA2-AES**	UDP	Throughput.scr	0.141	11.604	0.6894
AP1	**WPA2-AES**	UDP	Throughput.scr	0.161	11.257	0.7107
AP2	**Open**	TCP	High_Performance_Throughput.scr	0.463	19.738	0.2533
AP2	**Open**	TCP	High_Performance_Throughput.scr	0.418	17.734	0.2819
AP2	**Open**	UDP	Throughput.scr	0.224	13.774	0.3630
AP2	**Open**	UDP	Throughput.scr	0.203	13.289	0.3763
AP2	**WPA-TKIP**	TCP	High_Performance_Throughput.scr	2.032	20.395	0.2452
AP2	**WPA-TKIP**	TCP	High_Performance_Throughput.scr	0.207	21.242	0.2354
AP2	**WPA-TKIP**	UDP	Throughput.scr	0.234	14.19	0.3524
AP2	**WPA-TKIP**	UDP	Throughput.scr	0.234	14.415	0.3469
AP2	**WPA2-AES**	TCP	High_Performance_Throughput.scr	1.061	18.869	0.2650
AP2	**WPA2-AES**	TCP	High_Performance_Throughput.scr	2.255	17.824	0.2805
AP2	**WPA2-AES**	UDP	Throughput.scr	0.271	13.64	0.3666
AP2	**WPA2-AES**	UDP	Throughput.scr	0.277	14.892	0.3358
AP3	**Open**	TCP	High_Performance_Throughput.scr	0.106	19.753	0.3038
AP3	**Open**	TCP	High_Performance_Throughput.scr	0.109	19.578	0.3065
AP3	**Open**	UDP	Throughput.scr	0.37	14.09	0.4258
AP3	**Open**	UDP	Throughput.scr	1.046	12.279	0.4886
AP3	**WPA-TKIP**	TCP	High_Performance_Throughput.scr	0.073	18.617	0.3223
AP3	**WPA-TKIP**	TCP	High_Performance_Throughput.scr	0.331	18.255	0.3287
AP3	**WPA-TKIP**	UDP	Throughput.scr	1.142	10.028	0.5983
AP3	**WPA-TKIP**	UDP	Throughput.scr	0.163	12.741	0.4709
AP3	**WPA2-AES**	TCP	High_Performance_Throughput.scr	0.453	18.226	0.3292
AP3	**WPA2-AES**	TCP	High_Performance_Throughput.scr	0.415	18.235	0.3290
AP3	**WPA2-AES**	UDP	Throughput.scr	0.165	12.774	0.4697
AP3	**WPA2-AES**	UDP	Throughput.scr	0.224	12.52	0.4792

Appendix B: Latency Test Data

Device	Security	Protocol	Script Name	Average Response Time (ms)
AP1	**Open**	UDP	Response_Time.scr	0.001
AP1	**Open**	UDP	Response_Time.scr	0.001
AP1	**Open**	TCP	Response_Time.scr	0.001
AP1	**Open**	TCP	Response_Time.scr	0.001
AP1	**WPA-TKIP**	UDP	Response_Time.scr	0.002
AP1	**WPA-TKIP**	UDP	Response_Time.scr	0.001
AP1	**WPA-TKIP**	TCP	Response_Time.scr	0.001
AP1	**WPA-TKIP**	TCP	Response_Time.scr	0.001
AP1	**WPA2-AES**	TCP	Response_Time.scr	0.002
AP1	**WPA2-AES**	TCP	Response_Time.scr	0.002
AP1	**WPA2-AES**	UDP	Response_Time.scr	0.002
AP1	**WPA2-AES**	UDP	Response_Time.scr	0.002
AP2	**Open**	UDP	Response_Time.scr	0.001
AP2	**Open**	UDP	Response_Time.scr	0.001
AP2	**Open**	TCP	Response_Time.scr	0.002
AP2	**Open**	TCP	Response_Time.scr	0.001
AP2	**WPA-TKIP**	UDP	Response_Time.scr	0.002
AP2	**WPA-TKIP**	UDP	Response_Time.scr	0.002
AP2	**WPA-TKIP**	TCP	Response_Time.scr	0.001
AP2	**WPA-TKIP**	TCP	Response_Time.scr	0.001
AP2	**WPA2-AES**	UDP	Response_Time.scr	0.001
AP2	**WPA2-AES**	UDP	Response_Time.scr	0.002
AP2	**WPA2-AES**	TCP	Response_Time.scr	0.001
AP2	**WPA2-AES**	TCP	Response_Time.scr	0.001
AP3	**Open**	UDP	Response_Time.scr	0.002
AP3	**Open**	UDP	Response_Time.scr	0.002
AP3	**Open**	TCP	Response_Time.scr	0.001
AP3	**Open**	TCP	Response_Time.scr	0.001
AP3	**WPA-TKIP**	UDP	Response_Time.scr	0.002
AP3	**WPA-TKIP**	UDP	Response_Time.scr	0.002
AP3	**WPA-TKIP**	TCP	Response_Time.scr	0.002
AP3	**WPA-TKIP**	TCP	Response_Time.scr	0.002
AP3	**WPA2-AES**	UDP	Response_Time.scr	0.002
AP3	**WPA2-AES**	UDP	Response_Time.scr	0.002
AP3	**WPA2-AES**	TCP	Response_Time.scr	0.002
AP3	**WPA2-AES**	TCP	Response_Time.scr	0.002

References

[1] – University of New Hampshire Interoperability Laboratory. WLAN Consortium. http://www.iol.unh.edu/services/testing/wireless

[2] - P3 International KILL-A-WATT Electricity Usage Monitor http://www.p3international.com/products/special/P4400/P4400-HG.html

[3] – D. Becker, “Wi-Fi Takes Over in Homes,” 2005 http://www.news.com/Wi-Fi-takes-over-in-homes/2100-1010_3-5544025.html