White Paper

Cisco Aironet Access Point Wireless Security Module (WSM)

Executive Summary

With the rapid growth of wireless for day-to-day business needs, the discussion of how best to monitor and secure the corporate wireless network is gaining considerable traction. The topic becomes even more crucial when you factor in the sheer number of devices that are connecting - and the fact that many people use two to three wireless devices at the same time.

To monitor and secure a wireless network effectively, you must:

- Understand in real-time the quality of the available wireless connection anywhere in your network
- Identify devices within your network that could interfere with the quality of the wireless connection
- Isolate and proactively avoid any source of interference
- Identify devices enabling an unsecured opening in your network, whether they are accidentally or maliciously doing so
- Continuously scan for network attacks and proactively contain and mitigate these attacks
- Identify the location of devices within the network, including client devices and sources of interference or threats to the network

The traditional approach to monitoring and securing the network is to deploy a dedicated overlay of wireless access points interspersed with the access points that your corporate users use daily. The function of these dedicated access points - often referred to as “monitor mode access points” - is to listen to all channels on the 2.4- and 5-GHz bands. Depending on the vendor’s solution, the information gleaned from listening is used to analyze the state of wireless connectivity (typically signal strength), as well as to identify potential security threats.

This dedicated overlay comes with obvious costs:

- Cost for the additional access points
- Cost for additional Ethernet cabling infrastructure
- Ethernet port at the upstream access layer switching device
- Operational costs of managing additional access points

The Cisco Aironet® Access Point Wireless Security Module (WSM) for the Aironet 3600 and 3700 Series Access Points introduces a new way for customers to design and deploy their wireless networks. By tightly coupling data connectivity, spectrum analysis, and security threat detection and mitigation into a single, multipurpose access point, this new Cisco® solution eliminates the need for two separately deployed networks.

The 3600 and 3700 Series Access Points eliminate three out of four cost elements associated with a dedicated overlay while dramatically reducing additional costs. Together, the Cisco Aironet 3600 or 3700 Series and the Cisco WSM module dramatically simplify how customers can deploy, monitor, and secure their enterprise-class wireless network. This solution shifts the focus from questions such as how many extra access points are required, the role they will serve, and where to deploy them to how best to serve the business needs of corporate users through a high-quality and secure connection.

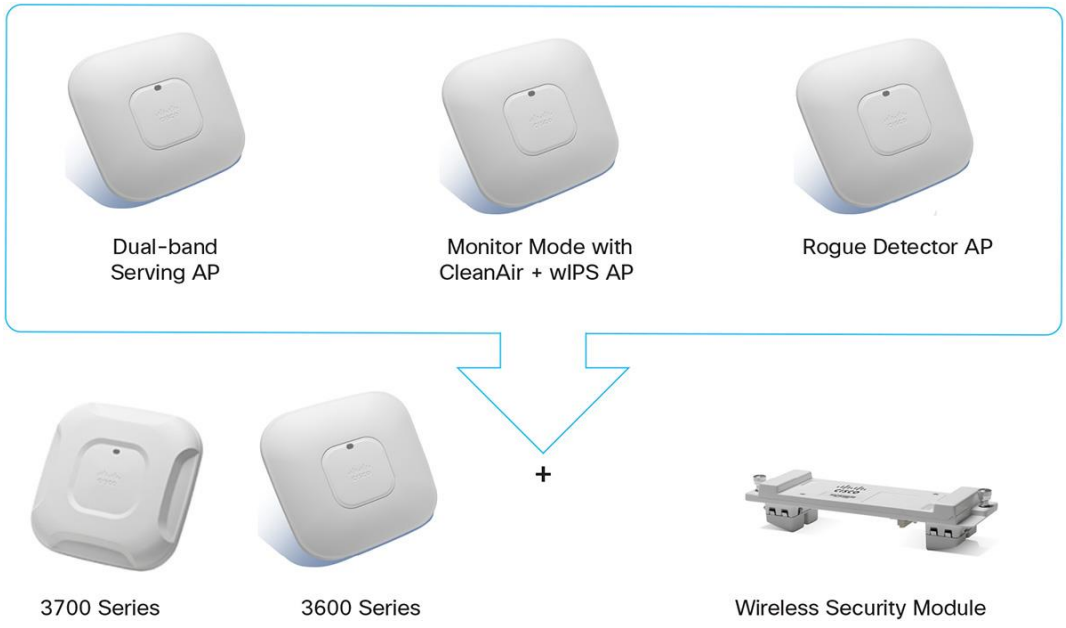
Technology Overview

The modular architecture of the Cisco Aironet 3600 and 3700 Series Access Points help you future-proof your wireless network deployments and maximize your return on investment by field-upgrading the access point using the feature-specific Wireless Security Module (WSM). The 3600 and 3700 Series with the WSM provides:

- Wireless data serving, spectrum monitoring, and security threat detection and mitigation - all in a single access point (the only access point in the industry to do so)
- Reduced total cost of ownership - 30 percent savings by eliminating the extra Ethernet infrastructure previously required together with an aggressive product price point
- Always-on security monitoring - 7/24 Interference analysis and threat detection and mitigation for all channels in 2.4- and 5-GHz bands
- Zero-touch configuration - Install, power-up, and go with no configuration required

As Figure 1 illustrates, the 3600 and 3700 Series integrates all data serving capabilities monitor mode with wireless intrusion protection system (wIPS) in a single device, the first such access point in the industry to do so.

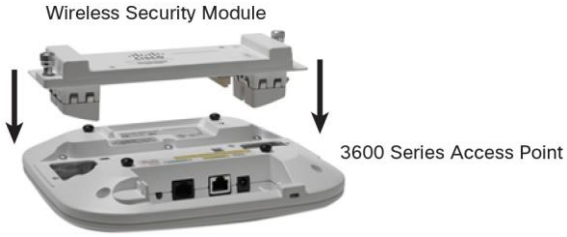
Figure 1. Multiple Functions Integrated in the Cisco Aironet 3600 and 3700 Series Access Points with WSM



The WSM is a completely self-contained wireless radio supporting both the 2.4- and 5-GHz bands with four integrated antennas, which are used to listen (Rx) to all channels on 2.4 and 5 GHz. The module does not transmit (Tx), and is therefore categorized as a 0 x 4:3 radio, as compared with the 4 x 4:3 characteristics of the integrated radios within the 3600 Series access point.

The WSM is physically inserted into the bottom of a 3600 or 3700 Series (integrated or external antenna version) and draws its power from the access point. Once the access point is powered up, the WSM automatically becomes the access point's third active radio and appears as the third radio slot (radio) of the access point on the Cisco Wireless LAN Controller that is managing the 3600 or 3700 Series access point. Figure 2 shows the WSM along with 3600 Series Access Point. The WSM fits similarly into the 3700 Series Access point.

Figure 2. WSM Along with 3600 Series Access Point



There is absolutely no configuration required by the customer to enable the WSM. Once the module is powered up, the following capabilities are automatically offloaded from the integrated radios and are executed on the WSM:

- Cisco CleanAir® technology monitoring for spectrum interference
- Wireless Intrusion Prevention System (wIPS) scanning for network attacks and malicious behavior
- Rogue detection
- Location context-awareness
- Radio resource management (RRM)

All of these capabilities run concurrently and are applied to all channels on both 2.4- and 5-GHz bands. Once the WSM is up and running, the integrated 2.4- and 5-GHz radios of the 3600 Series access point focus primarily on serving wireless clients and managing their data traffic.

Prior to the WSM, customers had two options when it came to enabling wireless security and spectrum monitoring: they had to deploy either enhanced local mode (ELM) or monitor mode (+wIPS). Both of these options enable the same set of integrated features we have touched on but with a different scope of coverage and associated cost. The WSM merges the best of these deployment modes with attractive pricing to offer up the best possible combination of feature richness and cost of deployment, as summarized in Table 1.

Table 1. Evolution of Wireless and Security Spectrum Monitoring

	Good	Better	Best
Features	Enhanced Local Mode	Monitor Mode AP	AP3600 or AP3700 with WSM Module
Deployment Density (#WSM: #AP)	1:1	1:5	1:5 - CleanAir 2:5 - wIPS
Serving Wireless data clients while Securing and Monitoring	Y	N	Y
Shared Ethernet Infrastructure for Wireless Data and Monitoring	Y	N (Requires a separate Ethernet connection for a Data AP and for Monitoring AP)	Y
wIPS Security Scanning	· 7x24 **On-Channel** · Best effort Off-Channel	· 7x24 **All Channels** on 2.4 and 5 GHz	· 7x24 **All Channels** on 2.4 and 5 GHz
CleanAir Spectrum Intelligence	· 7x24 **On-Channel**	· 7x24 **All Channels** on 2.4 and 5 GHz	· 7x24 **All Channels** on 2.4 and 5 GHz
Feature off-load - eliminating jitter from off channel scanning	N	N	Y

The WSM is a separately purchased hardware product, that can be installed into existing deployments of the 3600 or 3700 Access Points or purchased at the same time 3600 or 370are themselves purchased.

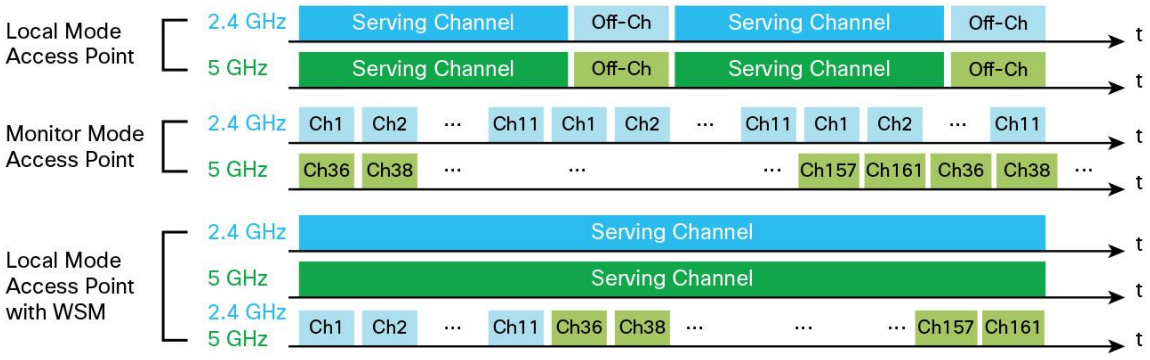
wIPS Functionality

Cisco Adaptive Wireless Intrusion Prevention System (wIPS) detects wireless-specific attacks. The WSM enables a local mode access point dedicated to serving clients to also behave as a monitor mode access point performing wIPS scanning on all channels, without affecting the access point's performance for serving clients.

Attack Detection Time Comparison

In local mode with the wIPS submode enabled, the access point is continuously monitoring the serving channel for any wIPS attacks and sporadically going off channel to detect any off-channel wIPS attack. In monitor mode with wIPS submode enabled, the access point's 2.4-GHz and 5-GHz radios simultaneously monitor both bands and sequentially visit different channels on the respective bands. As explained earlier, an access point with a WSM has both the primary radio dedicated to serving clients and the WSM visiting channels on both bands sequentially. Note that the WSM is dual-band module but operates on one band at a time. Figure 3 illustrates this scanning behavior for different access point modes. It should be noted that the off-channel scanning is a lower-level operation that does not impact client traffic.

Figure 3. Scanning Procedure with Different Access Points



We compared the attack detection time for the above access point modes. The representative results are shown Table 2. Note that detection time depends on the type of attack; the values listed in the table may vary for specific attacks. In the setup, the serving channels of the local mode access point and the local mode access point with WSM were the same. The on-channel attack was carried out on the serving channel. The off-channel attack was carried out on a random nonserving channel. The reported characterization is an average over multiple iterations of multiple attacks.

Table 2. Attack Detection Time Comparison between Different Access Point Modes

Channel of Attack	Local Mode Access Point	Monitor Mode Access Point	Local Mode Access Point with WSM
On-channel attack	T	~2T	T (Detected by primary radios)
Off-channel attack	>10T' (In some cases attack was not detected)	T'	~2T' (Detected by security module)

The experiments showed that for the on-channel attacks, the attack is detected by the primary radios. Hence the time to detect the attack for a local mode access point with WSM is similar to the time to detect the attack for a local mode access point without WSM.

As Table 2 shows, off-channel attacks usually take a long time to be detected by a local mode access point. This is because an access point in local mode is not able to dwell sufficiently long on the nonserving channel to collect enough packets to quickly detect the attack.

Such attacks are readily detected by a monitor mode access point, which is continuously scanning different channels. However, the local mode access point with WSM allows the access point to detect off-channel attacks in a way similar to a monitor mode access point placed at that location.

The results also indicate that when compared to a monitor mode access point, the WSM detection time for an off -channel attack takes twice as long as that of a monitor mode access point. This is because the monitor mode access point has the two primary radios scanning the two bands, while the WSM has a single radio to support both 2.4- and 5-GHz bands. However, when two local mode access points with WSM were used in the off-channel attack case, the attack detection time was reduced to approximately 1.2T'.

For wIPS deployment, the current deployment guideline is to use one monitor mode access point for every five local mode access points In order to get similar detection times we recommend that two out of five local mode access points should be equipped with the WSM. For better detection times, use more local mode access points equipped with WSM.

Coverage Comparison of WSM with Primary Radios

The received signal strength indicator (RSSI) represents the value in dBm of the signal strength at which a wireless packet is received. Figure 4 shows the scatter plot of approximately 200 RSSI values received at the WSM and primary radio collected from different points. The primary radio is the internal radio of Cisco Aironet 3600i.

Figure 4. RSSI Comparison between WSM and Primary Radio

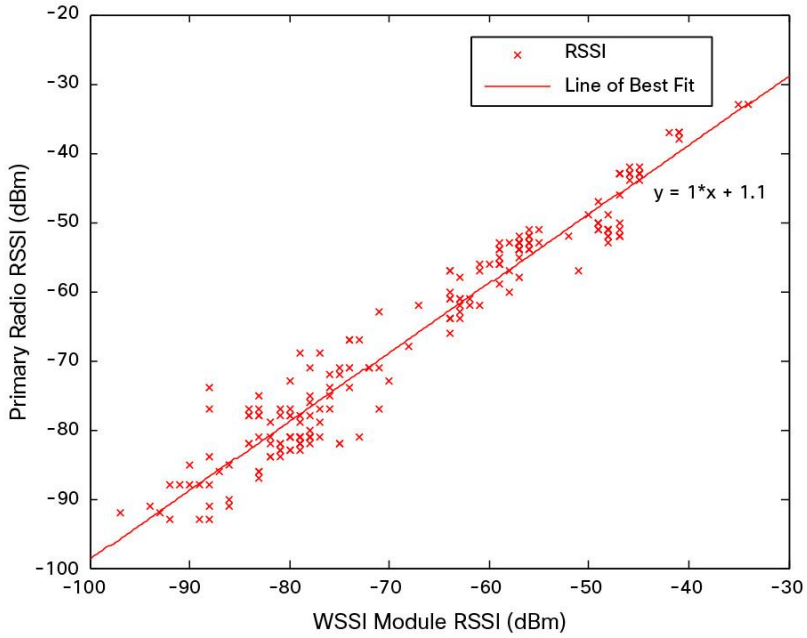


Figure 4 shows the high degree of correlation between the RSSI for the two radios. On average, the RSSIs received by the primary radio are about 2 dB stronger than the corresponding RSSIs from the WSM. This clearly indicates that the WSM has similar coverage to that of the Cisco 3600i access point.

Cisco CleanAir Offloading

The WSM module provides additional flexibility with respect to Cisco CleanAir solutions. When the access point is in local mode, the WSM will monitor both bands and collect CleanAir information while the primary radios are serving clients. More specifically, the detection and reporting of Air Quality (AQ) and Interference Device Reports (IDR) will be handled by the WSM.

We compared the detection of Bluetooth devices by an access point3600i (named SJC14-21A-Dungeness-E the screenshot shown in Figure 5) in monitor mode against an access point 3600i (named SJC14-21A-AP-Dungeness-X) in local mode with an attached WSM. Both access points are located next to each other and SJC14-21A-AP-Dungeness-X was serving regular client traffic. The new code release supporting the WSM allows for each reported interferer to be stamped with the “radio slot #,” which allows for the direct comparison of reports from different radio slots.

Interestingly, the relative RSSIs of each detected device remain consistent between the primary radios of the monitor mode access point and the WSM. The WSM offers very comparable interference device detection to that of the primary radios on the monitor mode access point, as shown in Figure 5. When we compared multiple types of interferers, we consistently got comparable RSSI readings; however, in the interest of brevity, only Bluetooth interferers are shown in Table 3.

Figure 5. A Bluetooth Link (Transmitter/Receiver Pair) was Detected by Both the AP with a WSM (Named SJC14-21A-AP-Dungeness-X) and the Monitor Mode AP (Named SJC14-21A-Dungeness-E) without WSM at Similar RSSI Values

AP Name	Radio Slot#	Interferer Type	Affected Channel	Detected Time	Severity	Duty Cycle(%)	RSSI
SJC14-21A-AP-DUNGENESS-X	2	BT Link	unknown	Thu Nov 15 01:26:22 2012	0	1	-86
SJC14-21A-AP-DUNGENESS-X	2	BT Link	unknown	Thu Nov 15 01:27:05 2012	0	1	-59
SJC14-21A-DUNGENESS-E	0	BT Link	unknown	Thu Nov 15 01:26:22 2012	0	1	-83
SJC14-21A-DUNGENESS-E	0	BT Link	unknown	Thu Nov 15 01:27:38 2012	0	1	-59

The obvious advantage of the WSM is to provide spectrum intelligence on all wireless channels, through AQ reports and interference detection, while the primary radios continuously serve clients. Moreover, as seen in Figure 6, the average AQ reported by the WSM and those of the monitor mode access point is also very comparable. The channel 1 measurements from both access points are highlighted to show the similarity of average AQ levels between the access point WSM (SJC14-21A-AP-Dungeness-X in the figure) and the monitor mode access point (SJC14-21A-Dungeness-E). Once again, for brevity, only the AQ levels in the 2.4-GHz band have been presented, but similar results are seen in the 5-GHz band. Hence, the WSM can essentially provide comprehensive interference awareness similar to a dedicated monitor mode access point.

Figure 6. Comparison of AQ Levels for the 2.4-GHz Band Reported for WSM Access Points and Monitor Mode Access Points

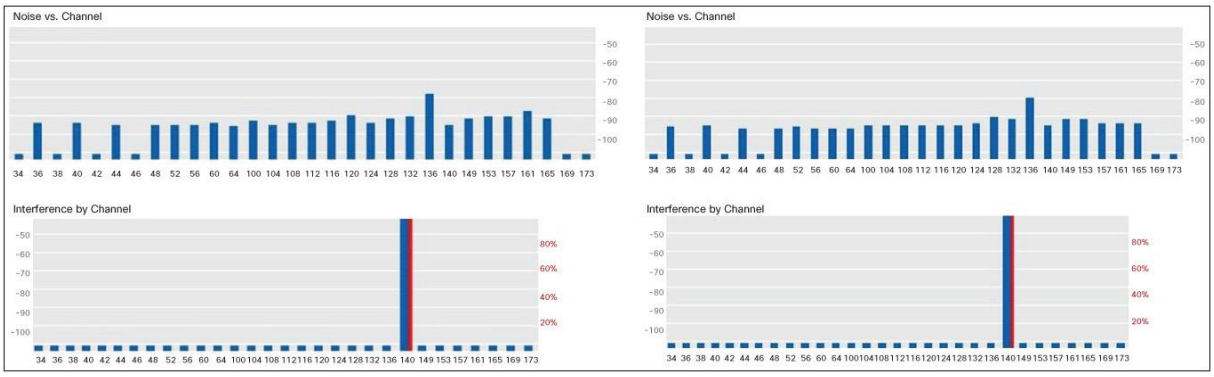
AP Name	Radio Slot#	Channel	Average AQ	Minimum AQ
SJC14-21A-DUNGENESS-E	0	1	96	92
SJC14-21A-DUNGENESS-E	0	2	93	90
SJC14-21A-DUNGENESS-E	0	3	90	87
SJC14-21A-DUNGENESS-E	0	4	89	85
SJC14-21A-DUNGENESS-E	0	5	89	86
SJC14-21A-DUNGENESS-E	0	6	93	87
SJC14-21A-DUNGENESS-E	0	7	88	80
SJC14-21A-DUNGENESS-E	0	8	81	72
SJC14-21A-DUNGENESS-E	0	9	84	74
SJC14-21A-DUNGENESS-E	0	10	86	77
SJC14-21A-DUNGENESS-E	0	11	95	86
SJC14-21A-AP-DUNGENESS-X	2	1	96	88
SJC14-21A-AP-DUNGENESS-X	2	2	90	86
SJC14-21A-AP-DUNGENESS-X	2	3	87	83
SJC14-21A-AP-DUNGENESS-X	2	4	88	83
SJC14-21A-AP-DUNGENESS-X	2	5	89	81
SJC14-21A-AP-DUNGENESS-X	2	6	95	80
SJC14-21A-AP-DUNGENESS-X	2	7	88	76
SJC14-21A-AP-DUNGENESS-X	2	8	83	68
SJC14-21A-AP-DUNGENESS-X	2	9	84	69
SJC14-21A-AP-DUNGENESS-X	2	10	87	73
SJC14-21A-AP-DUNGENESS-X	2	11	95	83

Radio Resource Management Offloading

In addition to its other activities, WSM collects radio resource management (RRM) metrics. This allows the primary radios to make fewer off-channel scans, thus ensuring they spend more time serving clients. Please note that the primary radios will still go off-channel to transmit neighbor messages; however, clients experience a more dedicated service since other off-channel functionality is offloaded to the WSM.

The RRM metrics collected by off-channel scans include interference, noise, and load. Figure 7 shows a comparison between these RRM metrics collected from a controlled testbed using a 3600 Series access point equipped with a WSM and a 3600 Series in monitor mode. Both these access points were placed in an anechoic chamber with a signal generator injecting a transmission on channel 140, with a transmit power of 12 dBm. As Figure 7 shows, the RRM statistics collected for noise, interference and load are very comparable between the access point with a WSM and those of a monitor mode access point. Once again, for brevity, only the results for channel 140 in the 5GHz band have been presented, but similar results are expected on other channels.

Figure 7. WiFi Interference and Noise As Reported by the AP3600 with a WSM (Left) and the AP3600 in Monitor Mode (Right) on the 5 GHz Band



Conclusion

The Cisco WSM allows the local mode access point to monitor all channels for wireless intrusion prevention system (wIPS) and CleanAir spectrum intelligence. The coverage area and other RRM parameter values of the WSM are similar to that of the primary radio in a 3600 or 3700 Series access point. The WSM also helps offload much off-channel functionality from the primary radio and thus allows for more dedicated service to clients.

The detection time for an off-channel attack is approximately two times that of monitor mode access point. Hence it is recommended that two out of every five access points be deployed with a WSM for wIPS deployment. For a non-wIPS deployment - for example, just CleanAir spectrum intelligence monitoring - one out of five access points can be deployed with a WSM. Note that the time to detect an interferer or an attacker improves as the WSM density increases.

For More Information

For more information about Cisco Adaptive Wireless Intrusion Prevention Solution, visit: http://www.cisco.com/go/wips.

For more information about the Cisco Self-Defending Network, visit: http://www.cisco.com/go/sdn.

For more information about the Cisco Mobility Services Engine, visit: http://www.cisco.com/go/mse.

For more information about the Cisco Unified Wireless Network, visit: http://www.cisco.com/go/wireless.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C11-723471-02 10/14