

## **SOHware White Paper Series**

WP100133

# **SOHware AeroGuard™ A MIMO Wireless LAN Technology**

Mike Mo, VP of Engineering

November 1, 2004

---

### Abstract:

The differentiating features and functionality of the **AeroGuard™ MIMO** solution ultimately provide a bottom-line benefit - a significant return on investment ("ROI"). SOHware's AeroGuard™ provides more network capacity with far fewer access points, resulting in cost savings, easy management, and reduced time to install, yet offers a higher WLAN performance across the enterprise premises.

## SOHware AeroGuard MIMO White paper:

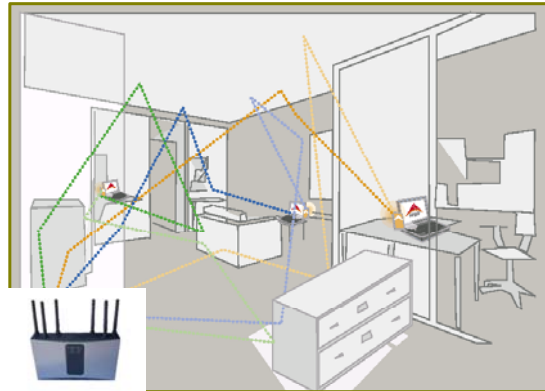
### 1. MIMO Transmission Overview

One of the latest WI-FI technologies available today is *multiple input multiple output* (MIMO), a smart antenna WLAN solution that has gained a very active center stage role in the future of wireless networking. MIMO can be simply explained as a multiple antenna system that utilizes rather than fights against the RF effects of multi-path, as shown in figure 1.

### ***MIMO means:***

#### ***Multiple Input - Multiple Output***

- Redefines the economics of wireless LAN technology.
- Optimizes the multi-path affect of radio signals as they reflect off surfaces in the environment.
- Unique multiple antenna system has the highest performance of any smart antenna signal processing.
- Removes remaining technical barriers to WLAN adoption



#### ***Result - greater range and capacity***

Figure 1- What is MIMO?

MIMO consists of multiple transmit and receive antennae, which divide one higher-rate data stream into multiple lower-rate data streams. Using complex signal-processing techniques, each of the lower-rate streams is then transmitted on the same channel, but through different transmitting antennae.

At the receiving end, MIMO takes advantage of something that is normally a liability for wireless networks; multi-path propagation. Multi-path is the way in which radio signals (RF) reflect off walls, ceilings, and other obstructions and then arrive with differing amounts of delay at the receiver. For conventional single antenna access points, these multiple incoming signals are wasted since only one signal can be processed at a time. MIMO technology, however, is able to process and recombine these multiple radio signals using complex algorithms and powerful DSPs, creating transmission efficiency and reception stability out of an object filled environment (think office space with typical partitions, walls and furniture).

Multiple antennae also make for improved antenna diversity and greater overall range. Each antenna receives its own version of the same data stream; some versions are more complete than others. Any data missing in one stream is more than likely available in the stream received by another antenna; thus, an increased amount of data enters the digital signal processor, more often than not resulting in a more accurate recombined data stream. Thus, where conventional access points will experience erratic connection quality at the edge of its reception radius, a MIMO access point provides a more stable connection and at

a further distance; ideal for streaming applications such as voice over Wi-Fi where latency can seriously affect application performance.

## 2. AeroGuard MIMO Overview

SOHware’s AeroGuard™ all wireless MIMO solution is based on Airgo Network’s True MIMO™ technology. Utilizing True MIMO™, AeroGuard™ yields an extremely high bit rate and extended range performance over conventional Wi-Fi access points, yet is fully backward compatible with current 802.11a/b/g clients. AeroGuard™ MIMO AP and complimentary MIMO CardBus are a wireless pair, operating at up to 108Mbps in a single 20 MHz single channel, and offer the wireless LAN industry’s only MIMO solution designed specifically for business-class applications.

AeroGuard™, in targeting business markets, would not be complete without advanced manageability, and again, exceeds conventional standards with a fully scalable, 3-layered management architecture that includes an enterprise NMS solution. AeroGuard™’s management design includes the best aspects of distributed and centralized management to maximize redundancy, scalability and efficient multi-site remote management. The three layered network architecture design is depicted in figure 2.

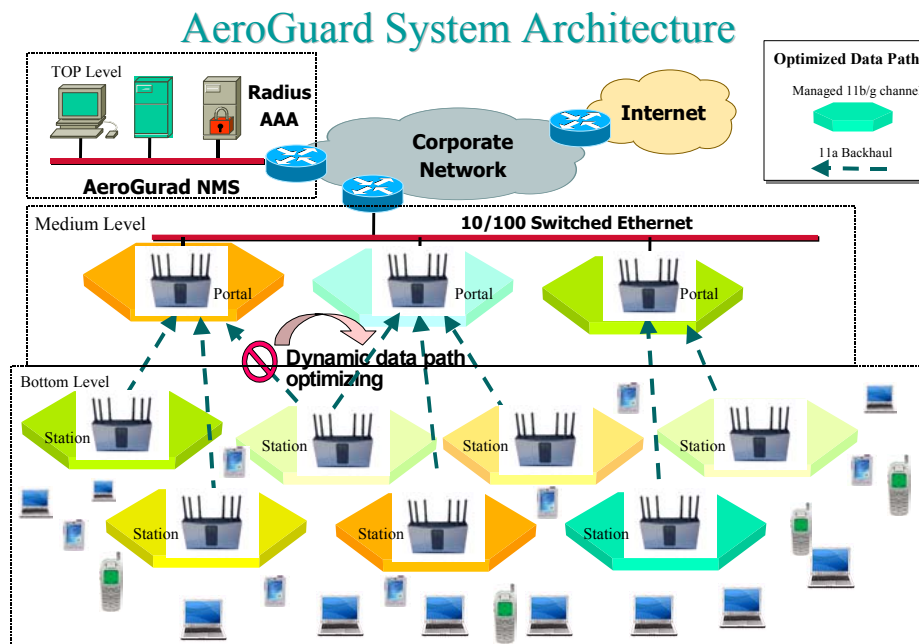


Figure 2- AeroGuard MIMO is a 3-layered architecture

Layer-1 is where AeroGuard Network Management System (ANMS) resides, which allows the business IT or service VAR complete remote monitoring and diagnostics of 1 or multiple locations where AeroGuard™ APs are deployed. Layer-2 highlights an integral feature within each AeroGuard™ AP, the Management Portal function, which can be enabled to provide aggregation of the wireless LAN domain (or subnet) and centralize the control of policy and RF distribution among all AeroGuard™ APs in the domain. Each Management Portal supports 20 station APs. This distributed intelligence allows more efficient queries and WLAN diagnostics of an entire network from the centralized NMS operations center. Layer-3 consists of the deployed AeroGuard™ station APs within each network domain, each

of which includes embedded routing intelligence that selects the best data path, if using AeroGuard™'s wireless backhaul feature, to the Layer-2 Management Portal AP. The APs are the linkage point for wireless equipped PDAs, tablets, and notebooks supporting typically from 40-100 clients depending on the application demands of the user.

### 2.1 AeroGuard Network Management System Features

The Layer-1 components reside in the Network Operation Center (NOC), consisting of an ANMS server and ANMS Client. The NOC usually co-hosts the Radius server on the same network.

ANMS is a powerful client server application with a rich set of features for managing large, single or multi-location wireless LAN (WLAN) networks. ANMS software was designed as part of a suite of True MIMO™ based wireless products that deliver unparalleled range, performance and ease of use to the campus/enterprise WLAN or branch office, and deliver robust and reliable performance throughout the WLAN coverage area.

ANMS can be deployed as a single location solution, or scale to multiple locations that manage diverse user populations and have stringent management and security requirements. Its flexible architecture permits a wide array of configurations to meet the needs of a growing organization.

ANMS features are shown in figure 3. This enterprise grade ANMS server is designed for large network deployment, using MySQL or Oracle DB as its database. As for authentication, currently we support Microsoft or Funk Radius server. The user interface is Java-based GUI (Java Server Pages), with minimum integration work needed. Northbound protocols were used when talking to external Network management system such as HP Open view (ANMS support SNMP, SQL, XML and CORBA interface). Southbound protocols via SNMP, CLI, WEB when talking to multiples of Portal APs.

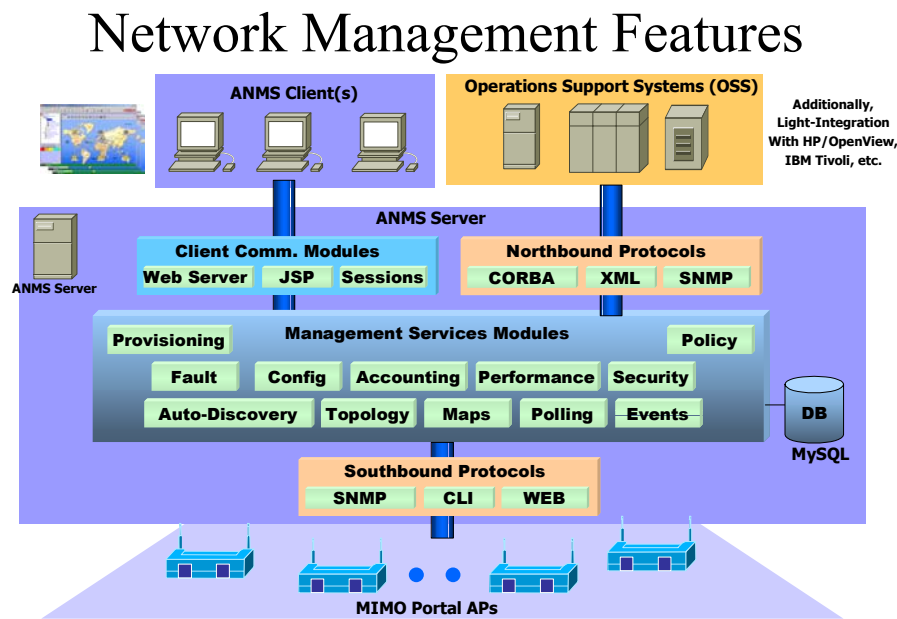


Figure 3 - ANMS block diagram

In short, ANMS encompasses all the four key functionality required for managing a WLAN:

*Wireless security management:*

AeroGuard ANMS provides secure verification of AP identity, which restricts network enrollment to known AP's only. The system allows the network manager to set up security parameters for user access to the wireless network. ANMS detects rogue APs and external attacks and intrusions, pinpoints the problem and alerts the system operator to the exact nature of the security attack.

*Network performance monitoring and management:* The performance management features provide real-time information about network health and assist in identifying any potential network problems before they move into a lost or alarm state. Detailed plots provide visual assessment and performance trend identification. ANMS automatically diagnoses, troubleshoots and repairs a wide array of error conditions before the WLAN can be affected.

*Global, centralized management of all WLANs:* ANMS can be used as a centralized management system for any size wireless network, from a small, single office deployment up to large, multi-site distributed WLANs. Furthermore the system provides excellent support for managed network service delivery by Value Added Resellers and Network Integrators.

*Network planning, configuration and deployment:* ANMS allows you to automatically scan the network and conduct the AeroGuard AP discovery. The resulting network topology map presents a powerful representation of channel usage and communication links. Furthermore, ANMS enables the automatic distribution of configurations and firmware upgrades to AeroGuard APs throughout the network.

## **2.2 Layer-2 Management Portal function**

The medium-level portal APs (to be viewed as station AP controller, or master AP) are connected to the 10/100 Ethernet network via Category 5 wire. Besides provides network physical link to a group of APs, also will serve its clients within 100 feet radius. (Side note on AeroGuard AP: Portal AP is identical to station AP, only difference is when "portal" status assigned by user, this distributed management function will be activated)

The portal AP's Network Management (NM) Portal Services provide a rich set of network management functions. Using the embedded NM Portal, Portal AP can operate in stand-alone mode to provide network management for a network of up to 20 AP's. The AP can also perform as a location or a branch manager working in conjunction with ANMS at the same ratio to the station APs. This is the scaled-down version of the ANMS, which is ideal for small or single-site application.

Whether configured as the network management server, or in use with ANMS, any AP can be set up as the portal or master AP and used to automatically distribute security policies, configurations and firmware upgrades to other AeroGuard APs on the network. In addition, the portal AP can also provide monitoring status of the managed APs and its wireless backhaul link status. As the result of this, enrollment, management, and security configurations of all APs can be done from a single location without the need for physical access to the APs.

Management Portal functions include:

- Policy management
- Secure enrollment of additional AP's into the network
- Embedded RADIUS server capabilities and authentication

- SYSLOG and diagnostic tools for monitoring and troubleshooting
- Backup and restoration of AP configuration data

Management support for the AeroGuard AP is available in four different interfaces:

- Web browser for basic and advanced AP configuration
- AeroGuard Network Management Portal for managing multiple APs
- Command Line Interface (CLI), accessible through a local 9-pin serial console port or over SSH

### 2.3 Station AP and Backhaul features

The bottom-level, station APs, via wireless interface and wireless back haul (a unique feature of this architecture, no wiring cost) will aggregate all traffic to each of the distributed Portal APs. The Station AP is often known as the stand-alone AP that acts and performs the typical functions of the traditional Access Points, except the AeroGuard AP contains additional feature sets that do not appear in other APs.

#### AeroGuard Station AP Software Feature Set

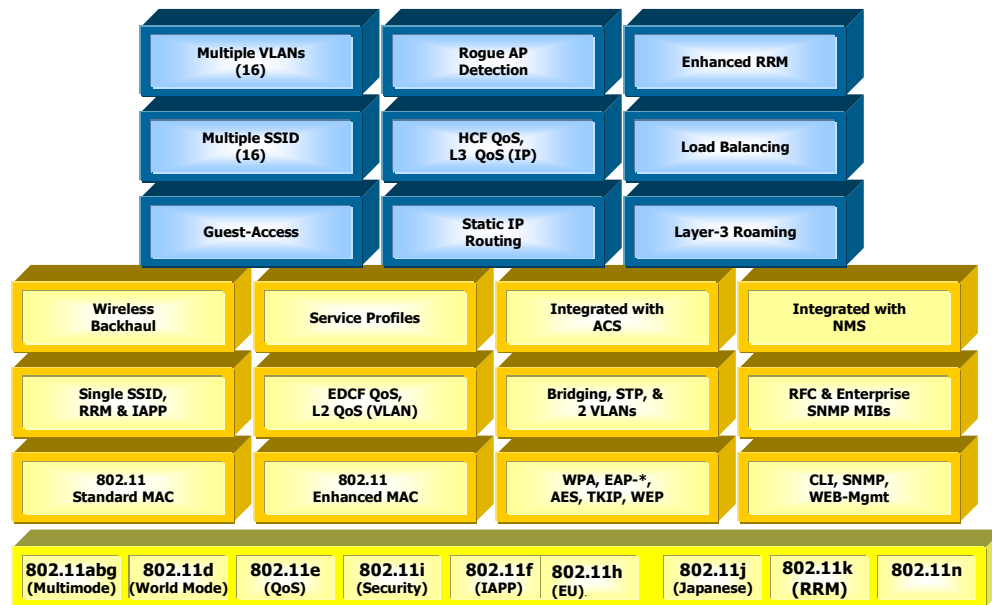


Figure 4: AeroGuard Station AP software feature set aimed at SMB/Enterprise market

The AeroGuard™ MIMO AP has enterprise grade features as shown in figure 4 above, its focus is towards application on large wireless network deployment, which in need of:

- **Multiple VLANs** -- AeroGuard APs support multiple VLAN by decoupling traffic flow and network services from the physical network topology, virtual LANs (VLANs) enable enterprises improve network traffic flow, increase load, and deliver varying levels of service and access to different groups of users.
- **Rogue AP detection** – The network management functions of AeroGuard portal AP NM include automatic network scanning and display all of the detected APs that potentially qualify as rogues.

- **Enhanced RRM** -- AeroGuard™ MIMO has extensive Radio resource management capabilities on radio channel, cell size and range.
- **Multiple SSID** -- AeroGuard™ MIMO using the multiple SSID feature. Users can access separate networks through a single physical infrastructure.
- **QoS (L2 & L3)** -- AeroGuard™ MIMO's Quality of Service features enable differential treatment of network traffic types to support special applications or extend priority access to designated groups of users. Eight classes of services (CoS) levels are available for assignment according to user or application based rules to give "best effort" priority according to the need in performance.
- **Load Balancing** -- Setting the loading of multiple AeroGuard™ MIMO station APs that are controlled by each AeroGuard™ MIMO portal AP.
- **Static IP Routing** -- IP routing adds flexibility to AP management and expands the addressing capability of the AP. User can specify static IP addresses outside the local subnet along with routing information to reach the addresses.
- **Layer-3 Roaming** -- AeroGuard™ MIMO support Layer-3 Roaming; which enable user do roaming cross-different subnet seamlessly (assuming radio coverage over both roaming subnet are continuous). Layer-3 mobility is a superset of Layer-2 mobility. An 802.11 client must perform Inter-Access Point Protocol (IAPP), a Layer-2 roaming, including AP discovery, before it can begin a Layer-3 roaming. Our feature set has an efficient proprietary Mobile IP implementation, the advantage is: no need to put agent in each client but only at AP side.
- **Service Profiles** -- As service profile is a set of attributes, including VLAN, COS, and encryption, applied to designated classes of users once a RADIUS authentication server authenticates them.
- **Single SSID RRM & IAPP** -- AeroGuard APs support the layer 2 roaming, i.e., 802.11f Inter-Access Point Protocol (IAPP).
- **Spanning Tree Protocol** -- AeroGuard APs support the spanning tree protocol.
- **WPA, EAP, AES, TKIP and WEP** -- AeroGuard APs offer comprehensive security solution that adheres to the industry standards and draft standards. For data encryption, AeroGuard supports WEP, Wi-Fi Protected Access (WPA) with TKIP or AES encryption. For User authentication, 802.1x authentication including EAP or WPA-PSK (pre-shared key). Furthermore, AeroGuard supports Microsoft Internet Authentication Server (IAS) and FUNK-RADIUS.
- **CLI, SNMP, and Web Management** -- the AeroGuard APs can be directly managed through three different interfaces: Command Line Interface via console port or SSH, Web browser interface, or via SNMP
- **Wireless Backhaul** -- AeroGuard™ MIMO wireless backhaul refers to the process of delivering data from a node on the wireless network back to the wired network. Some APs connect directly to the wired network, while others relay wireless signals from clients to the APs that are connected to the wired network, up to 5 levels of backhaul is allowed, which make a true "no wire" station AP deployment across a big campus of enterprise possible. Figure 4 below, illustrated the backhaul concept.

## Simultaneous AP and Backhaul

### *MIMO means more installation convenience and flexibility*

- Multi-mode - dual radio for simultaneous 802.11a and 802.11b/g bands
- Extends network coverage with no Ethernet wires
- Supports PoE where Ethernet is available

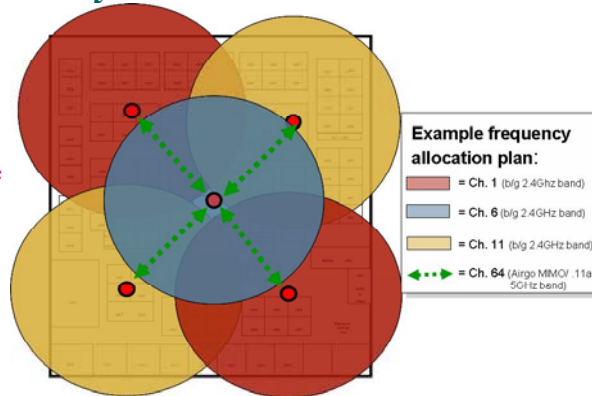


Figure 5 - Backhaul illustration of AeroGuard™ MIMO

In a nutshell, the SOHOfware AeroGuard™ MIMO, has rich enterprise features for control and maintenance, such as Secure AP enrollment and deployment, L2 Client Privacy, Secure “Staff” & “Guest” access, Portal page redirection, 802.1x: Internal/External authentication, Rogue AP detection, Policy-based management, Simultaneous 802.11a wireless backhaul b/g coverage, Real-time alarms and traps, Radio resource management, Supports 16 SSID & 16 VLAN, QoS controls (802.11e EDCA), Static IP Routing and dynamic RF path optimization (high availability feature when certain RF route is blocked due to external interference).

### 3. Enterprise-Grade Wireless LAN

As opposed to the consumer-grade Wireless LAN, enterprise-grade Wireless LAN excels in the Security, Management, Performance and Mobility. These 4 key criteria distinguish the products for mission-critical enterprise needs. Briefly re-capping these “must have” key points that is essential to enterprise WLAN.

#### 3.1 Security

WLAN without security, just like have a RJ45 jack in the parking lot, blindly granting open license for any one to the enterprise network, the results would be a disaster. Managing the security side of enterprise networks requires several things, namely:

- Protecting the ‘network’ from intruders
  - Requires authentication for users
- Protecting the Wireless DATA from sniffers
  - Requires some type of encryption
- Protecting you RF networks from being detected

- Requires network management feature to disable the SSID broadcasting, or set radio density high for smaller and controlled coverage.
- The ability to MANAGE WLAN users credentials
  - Includes WEP keys, users names, passwords, etc.
- Protecting wireless infrastructure from improper configuration
  - Required a good user manager interface on APs
- To dynamically assign user's IP address, gateway, etc.
  - Deploy DHCP server
- To let roaming users be authenticated by their original account and passwords
  - Requires authentication roaming features for authentication servers

### 3.2 Management

A management architecture that has centralized and automated management blocks is essential to enterprise network. Yet local distributed network management agent to do local management and monitoring also important as it improved the efficiency over all. The management of enterprise-grade WLAN, usually has two parts:

**RF Management:** Enterprises need to effectively harness RF and convert it into a reliable and predictable network medium (similar to wire-line networks), using statistical data gathered about channel reliability, throughput, interference, applications in use, user location, capacity, and possible network intrusion, to compute the best possible RF topology on the wireless network. With real-time RF management, enterprises can also use the air space to route around WLAN equipment failures, providing fault tolerance and network availability.

**Wireless Network Management:** Besides the radio related RF management, wireless network management covers the following 4 sub-categories:

- Network planning, configuration and deployment: Allows you to automatically scan the network and conduct the AP discovery. Also enables the automatic distribution of configurations and firmware upgrades to APs throughout the network.
- Wireless security management: Provides secure verification of AP identity, which restricts network enrollment to known AP's only. Detects rogue APs and external attacks and intrusions, pinpoints the problem and alerts the system operator to the exact nature of the security attack.
- Network performance monitoring and management: Provide real-time information about network health and assist in identifying any potential network problems before they move into a lost or alarm state.
- Global, centralized management of all WLANs: Centralized management system for any size wireless network, from a small, single office deployment up to large, multi-site distributed WLANs. Furthermore the system provides excellent support for managed network service delivery by Value Added Resellers and Network Integrators.

### 3.3 Performance:

An optimized radio resource management saves money. It will reduce interference, provides high availability, robust and resilient coverage, combining with QoS, it is a good enabler for current and future business applications.

Also, related to the "performance" topic. One thing worth mentioning is pre 802.11-n standard, for next generation of higher bandwidth throughput. Various vendors proposed smart antennas (called multiple input, multiple output, or MIMO) to improve signal quality, range, and data transfer rates of Wireless LAN access points and can greatly enhance bandwidth throughput, network availability and network coverage.

### 3.4 Mobility:

As more and more PDAs are equipped with wireless module, Voice over WIFI phones are gaining popularity, and most of the corporate laptops will ship with Wi-Fi embedded directly into the platform by 2005. As a business driver, wireless mobility within the enterprise will become a reality. Industrial answer to address this new demand is to implement Layer-2 (IAPP) and layer-3 roaming (Mobile IP).

Seamless roaming, which enable user do roaming cross-different subnet seamlessly (assuming radio coverage over both roaming subnet are continuous). Layer-3 mobility is a superset of Layer-2 mobility. An 802.11 client must perform Inter-Access Point Protocol (IAPP), a Layer-2 roaming, including AP discovery, before it can begin a Layer-3 roaming.

This features that will be greatly enhanced the usability and availability in enterprise environment. An enterprise wireless LAN should be ideally allow user to move between APs and cross subnets without losing their session and maintaining their authentication privilege.

## 4. AeroGuard™ MIMO excels on all the 4 categories

### 4.1 Security:

Comprehensive Security is provided via AeroGuard Network Management System (ANMS) that will ensure the integrity of mission-critical applications and data across the enterprise WLAN and support WEP and WPA v1.0 standards. Government-grade, 802.11i standard support is also provided with 256-bit key AES encryption and TKIP capabilities. AeroGuard provides the following additional security features:

- **The AeroGuard Security Portal** (*i.e.*, proxy RADIUS server) is integrated into each AP to perform user authentication functionality and to eliminate the need for an external RADIUS or other authentication server. The AeroGuard Security Portal provides automatic user key encryption generation on a per user or per session basis and supports the WPA 802.1x (*i.e.*, EAP-TLS) security standard.
- **Rogue AP Detection** functionality is provided where AeroGuard APs regularly scan their assigned radio frequencies and identify non-authorized APs ("rogue APs"). If a rogue AP is detected, then alarms are triggered within the ANMS console to alert IT Management.
- **Disable of SSID broadcasting** functionality is provided where AeroGuard APs disable the SSID broadcasting, so the not-intended neighboring wireless client does not see this AP.

### 4.2 Management:

**Advanced Network Management Software.** The ANMS is a centralized Web-based console that monitors, manages and maintains all the AeroGuard APs in the network,

regardless of the size of the network or the physical location of the APs. The ANMS has an open design that incorporates industry standards for easy integration with the existing IT infrastructure, including SNMP-based network management systems, such as HP OpenView, AAA servers (e.g., MS RADIUS IAS) and identity databases (e.g., MS Active Directory).

**Self-Configuration.** AeroGuard intelligent APs perform Self-Discovery functionality. Subsequent to their connection via a Power-over-Ethernet connection or an AC outlet, the nodes automatically detect the type of connection (*i.e.*, wireless link or Ethernet cabling). The APs then perform Self-Configuration functionality. During self-configuration, the AP automatically performs a self-test, radio channel scan and the selection of its function.

**Wireless Backhaul.** The AeroGuard APs can be configured to communicate solely with clients or in an All Wireless Networking ("AWN") mode, where APs can communicate with one another to perform the function of a wireless mesh backhaul and to eliminate costly-wired connections to each AP. The Awn provides an intelligent routing algorithm that enables the APs to select the most efficient path for the data transmission and to perform self-healing functionality in the case that an AP is disabled. It can be used for campus facilities, remote office or temporary WLAN deployments and significantly reduces labor-intensive, site survey costs.

#### 4.3 Performance:

SOHware **AeroGuard™ MIMO** provides increased data rates of up to 108 Mbps with an AeroGuard True MIMO™ multiple antenna, 802.11a- or 802.11g-based solution. Similarly, the maximum data rates of 54 Mbps are reliably provided at extended ranges of up to three and five times that of the typical WLAN technologies.

The **AeroGuard™ MIMO** solution also provides unequalled ease-of-use. The intelligent provisioning functionality (*e.g.*, auto-discovery and configuration and all-wireless backhaul networking) is well-suited for campus, remote office and temporary WLAN deployments. Additionally, the Web-based AeroGuard ANMS console provides for centralized monitoring, management and maintenance of the AeroGuard WLAN solution.

#### 4.4 Mobility:

**Seamless Mobility.** The AeroGuard MIMO ANMS provides seamless mobility features that enable layer-2 Inter-AP subnet roaming per the 802.11f standard. Additionally, wireless VLANs can be assigned on a per user, per port, per subnet or per protocol basis and clients can be automatically routed across multiple APs to support mobility needs. Layer-3 roaming also enable enterprise client roaming across different subnets without losing their session and maintaining their authentication privilege.

### 5. AeroGuard™ MIMO differentiation

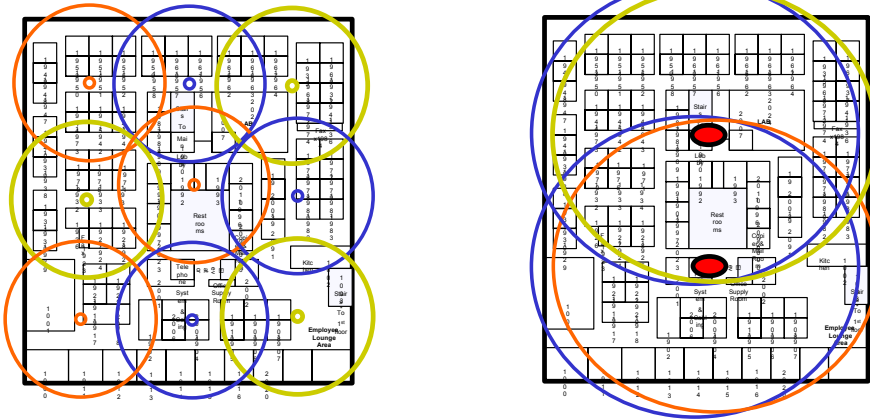
We provide the following differentiations, to ensure the best cost/performance ratio in the following areas for the enterprise-grade WLAN product:

#### 5.1 Superior Range

AeroGuard™ MIMO offers up to 4 times in coverage as compared to conventional coverage. Figure 5 illustrated, in this actual deployment, we only need two MIMO APs to cover 100 cubicles for an enterprise environment, as opposed to nine ordinary non-MIMO APs needed. Other deployment case studies, also in SOHware web site, clearly

showed the extended range characteristics of MIMO is well suited for many application such as enterprise network.

**Conventional AP deployment**      **True MIMO™ AP deployment**  
**9 Standard 11b APs @ 0.48 Mbps/user**      **2 AeroGuard MIMO APs @ 2 Mbps/user**

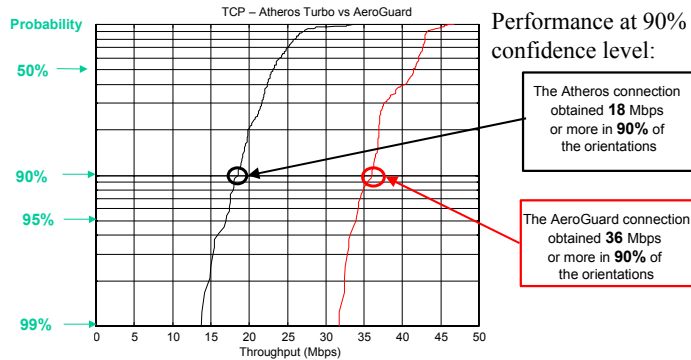


*An order of magnitude improvement in range and capacity!*

Figure 6 - Superior range of AeroGuard™ True MIMO

**5.2 Higher Throughput**

We have conducted TCP throughput put tests and PC magazine also conducted MIMO TCP throughput tests in August, 2004, AeroGuard™ MIMO offers 2 to 3 times in TCP throughput. As Figure 6 illustrated below, We have test MIMO in 802.11a Turbo mode (108Mbps) against an AP that is using Atheros based design running 802.11a Turbo mode (also 108 Mbps). The AeroGuard MIMO AP's TCP performance is consistently 2-3 times higher than non-MIMO AP.



(The charts plot the probability that the observed variable is less than or equal to the x axis. i.e. the y axis plots probability that the throughput is less than or equal to the throughput denoted on the x axis. )

Figure 7 – Comparative Performance

### 5.3 All Wireless, No-Wire Backhaul

AeroGuard™ MIMO wireless backhaul provide 3-5 levels of backhaul with easy. Which means, AeroGuard MIMO APs will reach 3-5 times more range of RF coverage than conventional APs without the cost of Ethernet wiring. This true “no-wire” AP deployment across a big campus of enterprise is 1<sup>st</sup> in the industry.

### 5.4 Spectrum efficiency

AeroGuard™ MIMO operates up to 108Mbps in a 20 MHz single channel, this is the only industrial True MIMO that has this 2 to 1 spectrum efficiency over other competitors. Other not true MIMO in the market uses 40 MHz per single channel, limiting the available non-overlapping radio channels.

## 6. Summary:

The differentiating features and functionality of the **AeroGuard™ MIMO** solution ultimately provides a bottom-line benefit—a significant return on investment (“ROI”). SOHware provides more network capacity with far fewer access points, resulting in cost savings, easy management, and no-wiring, yet high performance WLAN across the enterprise premises.

## References

1. AeroGuard Network Case Study, Dr. J. Gerry Purdy, Principal Analyst, MobileTrax Inc.