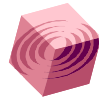


September 2004

24x7 Monitoring of 802.11 RF Medium for Network Performance, Reliability and Security

A Whitepaper by AirTight Networks, Inc.



AirTight
NETWORKS

339 N. Bernardo Avenue, Suite 200
Mountain View, CA 94043
www.airtightnetworks.net

"Air" is now a part of the corporate network. It must be monitored to ensure network security and maximize performance and reliability.

WLANs are gaining widespread acceptance due to the convenience and flexibility they offer to the end users. Business-critical applications are increasingly riding on WLANs in corporate offices, manufacturing floors, healthcare establishments, and even public hotspots, as wandering corporate laptops connect to corporate networks from these public WLANs. However, there are significant challenges in planning, performance monitoring of WLAN networks, as well as in securing these networks from wireless based attacks. Consequently, wireless networks need to be monitored and managed to achieve high performance, by ensuring high quality of communication over the wireless medium, good network coverage, and comprehensive protection against security breaches such as Denial of Service (DoS) attacks. There is also a need for enterprise grade troubleshooting tools to diagnose network performance issues and minimize network down time.

This white paper describes an approach to monitoring and troubleshooting of WLANs and introduces SpectraGuard™ Enterprise—a sensor based system from AirTight Networks to meet these requirements. SpectraGuard Enterprise continuously monitors the WLAN transmission medium to provide unprecedented visibility into security, reliability, and performance of the wireless network.

Wireless Networks Challenges

- Invisibility of the wireless medium makes it difficult to determine the network coverage at each point in the space.
- IEEE 802.11 'a' (5 GHz), 'b', and 'g' (2.4 GHz) frequency bands are unlicensed resulting in the possibility of multiple networks existing in the same space.
- Indoor wireless propagation is intercepted by building materials such as walls, windows, concrete columns, metallic objects, and even human density. This results in unpredictable and unreliable network coverage that is difficult to visualize.

The following phenomena pose additional challenges to monitoring of WLAN networks:

- Access points shut down, re-start, and their configuration is changed
- Client devices are constantly on the move and are shut down and restarted continuously
- New access points and clients are constantly introduced into the WLAN environment
- Objects in a building change their location. For example:
 - Movement of elevators
 - Relocation or movement of equipment or large furniture
 - Opening and closing of doors and windows
 - Changing human density (people gathering or dispersing)

These changes make the RF medium unreliable, affecting the WLAN network as follows:

- Fluctuation in network capacity resulting in low bandwidth for some users
- Transient faults, connections/disconnections, poor speed, and network outages

The first step in assuring a good quality WLAN is to provide the following:

- 24x7 visibility into network coverage and traffic patterns
- Troubleshooting and diagnostics to understand the root cause

WLAN Security Vulnerabilities

WLAN technology has significantly increased the vulnerability of corporate networks to network disruption and data theft attacks. Security threats from wireless based attacks can be broadly classified into:

- Rogue access points and mis-configured access points
- Mis-connections: Enterprise clients connecting to external networks, external clients establishing connectivity to an enterprise AP, and ad hoc networks
- Denial of Service attacks (DOS)

Traditional firewalls or intrusion detection systems, which provide protection from external threats in wired networks, do not address this vulnerability. Notably, the network is vulnerable even if there is no WLAN. A rogue access point can add wireless connectivity to your network for wrong reasons.

Good network performance also requires elimination of these threats for which 24x7 monitoring for visibility into ongoing wireless activity is mandatory (Ref: AirTight whitepaper titled, "WLAN Security—Why your Firewall VPN and IEEE 802 11i aren't enough to protect your network").

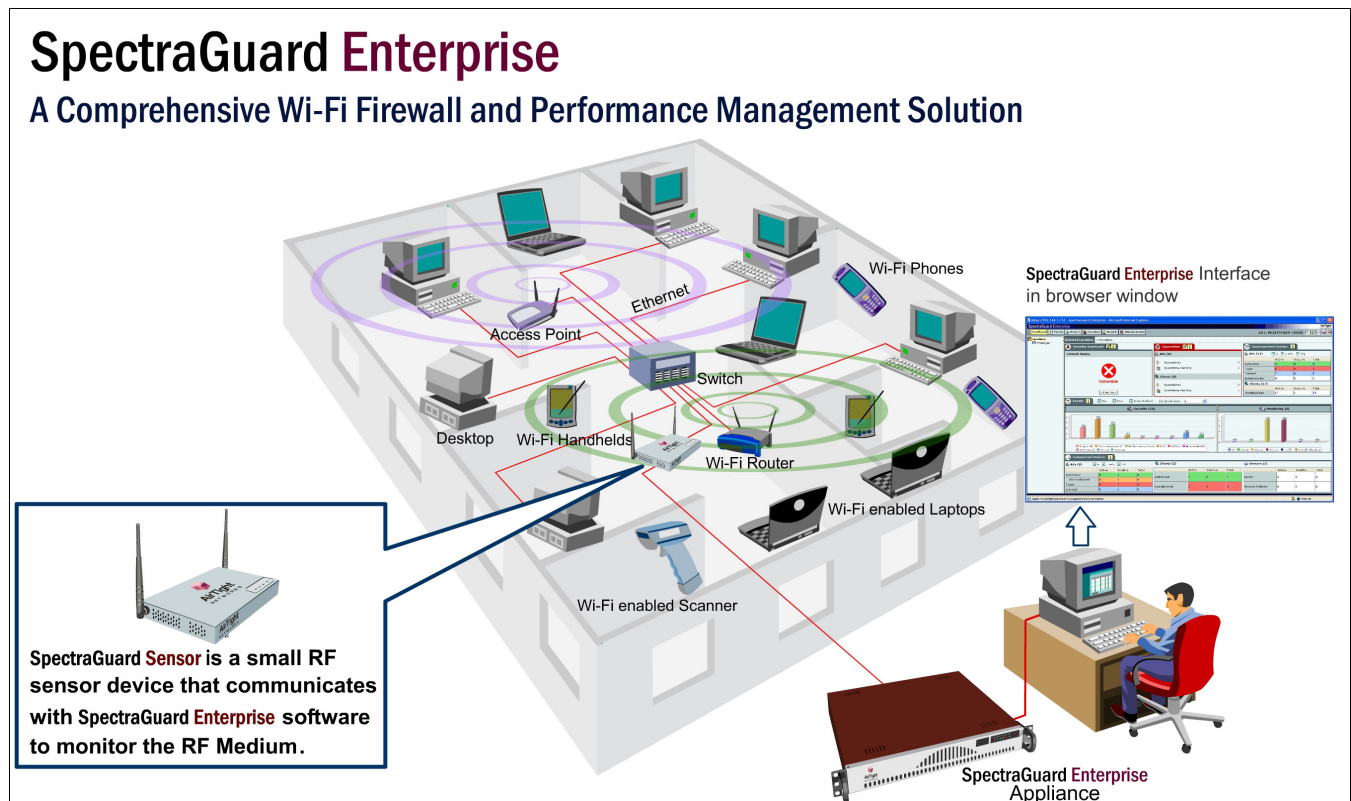
SpectraGuard Enterprise: 24x7 Monitoring of RF Medium

SpectraGuard Enterprise from AirTight Networks enables 24x7 comprehensive monitoring and troubleshooting of the RF medium to enable high performance and trouble-free operation of WLANs. Further, the monitoring can be done from a centralized location.

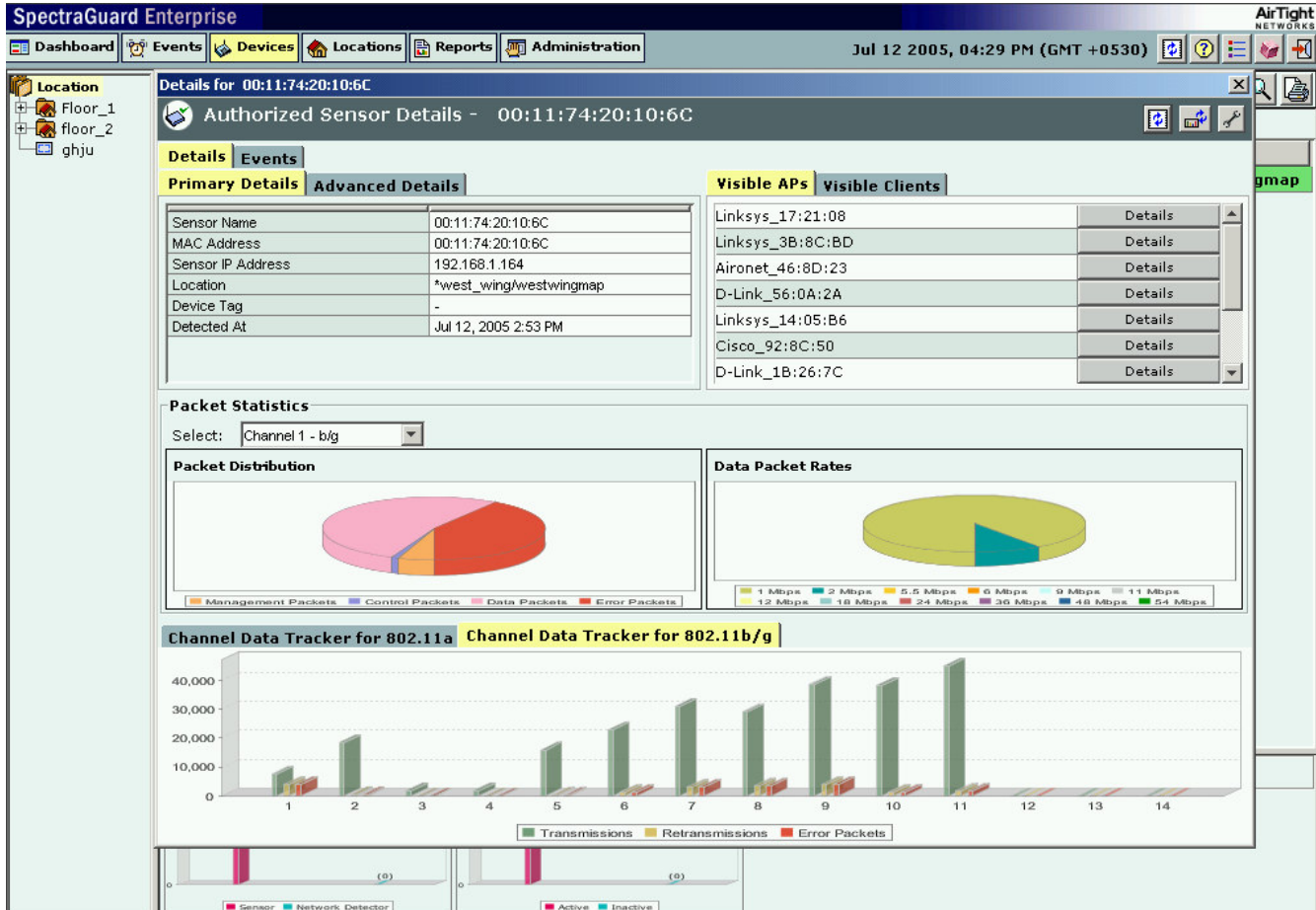
SpectraGuard Enterprise consists of a SpectraGuard Enterprise Appliance (Server) and SpectraGuard Enterprise Sensors (Sensors). Sensors detect and analyze WLAN activities over the RF medium and send data to the server. The server aggregates, correlates, and analyzes the data to provide insightful information about network coverage, security vulnerability, WLAN devices, and all WLAN devices' associations that are active. In the event of a security breach, the Server and Sensors protect the network by stopping all associations with the devices that are responsible for the breach. The system also helps locate the devices for physical remediation.

SpectraGuard Planner, a path breaking RF planning technology from AirTight Networks, can be used to plan access points and Sensors to ensure optimum network coverage and minimal security exposure. Monitoring for security often needs to cover larger space than monitoring for WLAN operation, which have to be scanned by Sensors.

RF planning is necessary to ensure that there is optimum network coverage while security exposure is minimized.



Network administrators interact with SpectraGuard Enterprise using its intuitive graphical interface that allows the administrator to define policies, get alerts regarding policy violations and performance degradations, create reports, review history of events, etc. Using this interface, it is possible to troubleshoot or analyze current or past problems of any remote location from a centralized monitoring center.



24x7 monitoring by SpectraGuard Enterprise enables better network performance and higher reliability by ensuring the following:

- Network Performance
 - Adequate coverage (signal strength throughout the space)
 - Avoidance of channel interference
 - Optimum client density per access point
 - Remote monitoring and management
 - Capacity provision and forecast for new applications
- Network Reliability
 - Access point redundancy
 - Protection against Denial of Service attacks
- Network Security (Protection from WLAN based attacks)
 - Detection of all security threats and complete prevention against each attack
 - Location of participating devices for physical remediation
 - 24x7 watch on the corporate air

Summary

- Unlicensed nature of 802.11 WLANs coupled with its affordability has resulted in proliferation of 802.11 networks. Further, the invisibility of the wireless medium makes it difficult to determine the network coverage at each desired point in space and the security exposure.
- Indoor wireless propagation is intercepted by building material such as walls, windows, concrete columns, metallic objects, and even human density. This results in unpredictable and unreliable network coverage that is difficult to visualize.
- Adequate network coverage, avoidance of channel interference, and optimum user density per access point are the key drivers to achieving high network performance.
- Prevention against Denial of Service attacks and centralized monitoring can help reduce network down time.

Centralized monitoring of WLANs and the IPS firewall capability of SpectraGuard Enterprise enable WLANs that deliver high performance, are reliable, and secured against all types of security threats.