

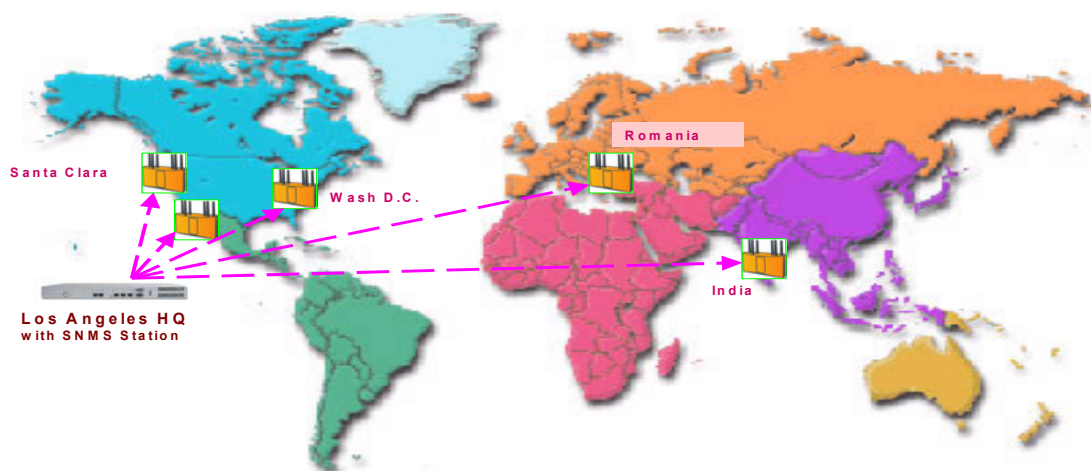
## **AeroGuard™ MIMO Centrally Managed All Wireless Solution for a Global Enterprise.**

**A Multi National Corporation, California, USA  
Corporate IT Department**

### **Application Scenario:**

A leading, global provider of high performance Internet Protocol network testing solutions, located in Southern California, USA, markets its products through a network of direct sales offices and distributors. These offices are spread through out the world. There is an office in Santa Clara, two in Washington DC, one in Research Triangle Park, North Carolina, one in India and two in Romania. All together, roughly 500 employees work in these locations.

The corporate head quarter in Southern California hosts all of the web servers, email servers, user authentication servers, and servers hosting design and test information. The distributed offices have high-speed Internet access with secure VPN connections between the branch offices to the corporate network. All network management and supervision is provided from the head quarter and often employees in various offices travel to other locations and need connectivity to the corporate network. Similarly, customers visiting each location require connectivity to their home site computers via the Internet.



**Figure 1: All Wireless Solution for a Hospital in the LA County**

## Desired Outcome:

The IT department wishes to maximize network connectivity for its mobile sales staff at each location. The goal was to extend seamless connectivity across the seven seas. Instead of the traveling employee spending their time looking for an Ethernet socket in a wall and a wire and wasting time reconfiguring their computers, a standardized configuration free corporate platform that is secure and could be managed head quarter was desired.

So the goal was to set up a wireless environment that would allow the mobile workforce to easily look up essential business data, send and receive emails, enter most current sales and market activity reports from the field, enhancing corporate productivity by saving valuable time while weeding out the connectivity frustration. The wireless infrastructure that is centrally managed for access control policy, configuration, performance management and maintenance were unanimously considered must-haves.

Needless to say that such environment needed to be, **secure**, configuration free and offer **unrestricted roaming from location to location**. Performance and affordability were at the top of the list of important criteria. With **minimum number of access points** of adequate capacity (bit rate, reach and coverage), support for 802.11x and 802.11i compliant AAA RADIUS, and AES encryption were also critical requirements. Ability to manage the entire distributed wireless environment, including **data security and user authentication from the head office was essential**.

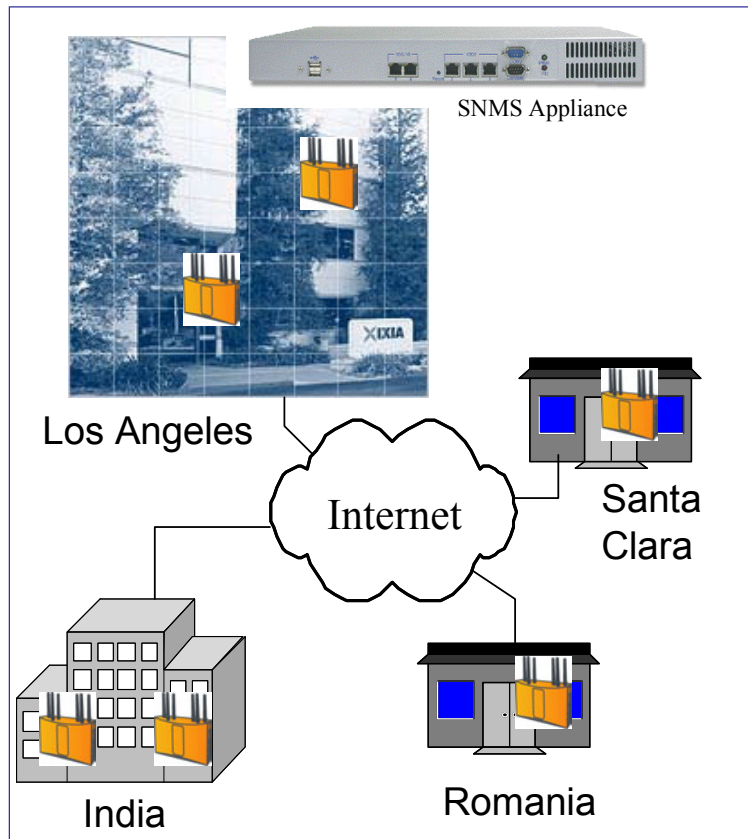
A wireless LAN solution that provides Enterprise class security and manageability, with the installation flexibility to easily adapt to varied building structures was important as building in different parts of the world are different. There is also lack of wiring infrastructure, limiting the options on location of the access point. These access points in each distributed office location had to be link over the Internet to a centralized management station located in the Southern California office for real-time remote monitoring, diagnostic and maintenance functions.

Several options were considered by the corporate IT department before settling on SOHware's high performance AeroGuard™ MIMO all wireless solution; a decision purely based on performance and best value for money.

## AeroGuard™ MIMO All Wireless Solution:

AeroGuard™ MIMO solution provided both wireless LAN at multiple global locations. The included AeroGuard™ Network Management Appliance

provided a fully scalable management system for the entire wireless environment.



**Figure 2: AeroGuard™ MIMO Managed Wireless Network**

The AeroGuard™ MIMO all wireless solution with superior performance; more bandwidth, increased range and coverage, and with wireless backhaul capability, as shown in Figure 2 above, was proposed. Due to its superior performance, better than **250 feet** coverage and ability to support **50 to 100 users**, the solution required very few access points compared with a traditional solution. Network Management Appliance located in the head quarter provided the necessary configuration, fault, and advanced radio frequency management and software upgrade capability.

The access points working at 108 Mbps for each radio offered enough resources, i.e. bandwidth, for a variety of the clients and applications. Although the maximum performance is available for MIMO compliant adaptors, the system is fully compatible with either 802.11g compliant 54 Mbps, if or 802.11b compliant 11 Mbps client cards, assuring maximum system performance to even with any mix of the two.

Among a host of security options available in the solution, **AES encryption** was utilized, making the wireless environment extremely secure. The solution fully supported their existing *AAA RADIUS server* for users authentication that even permitted visitors open access to Internet through the same wireless system without the fear of loss of privacy.

The conference rooms were given their own secure access via a separate SSID and VLAN arrangements, where visitors could also access the Internet but layer 2 privacy and isolation was maintained to disallow them the access to companies host computers. Other important features include:

- 802.11i compliant security
- Remote access control and user authentication
- Use of existing AAA RADIUS servers
- 802.1x: Internal/External authentication
- L2 Client Privacy, users not able to view other users' computer
- Simultaneous backhaul and access point coverage
- 16 SSID & 16 VLAN for segregating multiple workgroups
- Separation of "Corporate" & "Guest" access
- Secure enrolment & deployment of AP
- Rogue AP detection
- Real-time alarms and traps
- Extensive Radio resource management
- Remote software download and upgrades
- Policy-based security and access control
- QoS controls (802.11e) to support Voice over IP and Wi Fi

SOHware is proud to fulfill customer's desired outcome; more productive work environment through higher performance, very secure and yet affordable solution.