



Managing Your WiFi Network Through Thick & Thin: Keys to Successfully Managing Any Wireless LAN

EXECUTIVE SUMMARY

Your ability to effectively manage your wireless network depends not on whether you use 'thick' or 'thin' access points, but on the capabilities of your network management solution. Your selection of a hardware solution and network architecture should be determined by your operational requirements, budget, vendor support, and other factors. A good wireless management solution does not restrict your ability to select the best hardware available, but gives you:

- Flexibility to manage your wireless infrastructure no matter how large or complex it grows in the upcoming years
- Visibility to determine exactly how your network is being used and how it is performing at all times
- Usability for your entire IT staff rather than a select handful of highly trained engineers
- Security enforcement so you know your policies are in effect across your entire network at all times
- Strong return on your investment by reducing support costs, improving security, and delivering the performance your users need

The AirWave Wireless Management Suite software gives you total control over your entire wireless network infrastructure, whether you use 'thick' access points, thin APs, or a combination of both.

Introduction: The Thick and Thin of Wireless Management

Because the adoption of WiFi technology by enterprises, small businesses and home users alike has been so fast, it is sometimes easy to forget how young the technology is and how rapidly it continues to evolve. One of the most readily apparent industry changes in the past several years has been the introduction and rising popularity of the "thin AP" architecture in many enterprise environments.

There is a widespread misconception that the thin AP architecture has 'solved' the problem of wireless network management. It has not. In fact, because the organizations who are adopting thin AP architectures typically have larger wireless networks and denser deployments, their need for robust wireless network management is generally even greater than organizations with thick AP installations. Whether your wireless network can be managed efficiently and



centrally depends more on the capabilities of your network management system than on your hardware selection and network architecture. Before proceeding with a discussion and comparison of wireless LAN manageability, we must first define the two leading WiFi architectures today.

A **'thick'** (or 'intelligent') wireless access point is, in effect, a small wireless bridge with a WiFi radio, handling authentication, encryption, and the overall management of the client devices connected to it. Each thick AP is a stand-alone device with dozens of settings that must be configured and monitored via a network management application (or via a manufacturer-defined web UI in very small deployments). Almost all first-generation WiFi devices, such as the Cisco Aironet and Proxim ORiNOCO products, were thick access points – and these are still the top-selling products on the market today. Especially in small or remote office environments, these stand-alone access points often still have significant cost and performance advantages over "thin" products, which typically require a persistent connection to a controller in order to function.

A **'thin'** access point looks similar to a thick AP and may even share the same bill of materials. However, in a thin AP architecture, encryption, authentication, and policy settings generally occur on a central switch or controller, to which multiple thin access points are connected, rather than on the AP itself. The thin AP simply passes wireless network traffic to the switch, performing few complex tasks locally. Thin APs are sometimes called 'dependent' access points, since they often cannot function on a stand-alone basis without this central controller. One advantage of the 'thin AP' architecture is that it significantly reduces the number of devices that must be configured, since most network policies are set at the controller and far fewer settings need to be managed on a device-by-device basis. The thin architecture also offers certain advantages in roaming and fast hand-off, since it is easier to coordinate movement between two APs connected to the same switch than to coordinate hand-off between stand-alone devices. For these reasons, many organizations with dense campus RF environments and plans to implement wireless VOIP applications have begun to migrate from thick to thin AP architectures.

"Thick AP" deployments earned a reputation for being difficult to manage largely because the manufacturer-provided management solutions were clumsy and difficult to use. The thin AP architecture addressed some of these weaknesses by making configuration and firmware management slightly easier, since there are fewer devices to update and control. However, a good network management solution should automate most of these routine functions, regardless of architecture, making it simple to configure and control a network with hundreds or thousands of thick or thin devices. In the final analysis, network architecture alone has little impact on overall manageability.

As depicted in the table below, the selection of an appropriate wireless network management solution has less to do with the underlying architecture of the network than with the capabilities of the management solution itself:



Managing Your Wireless LAN Through Thick and Thin

Network Management Function	Role	Thick vs. Thin AP
User & device monitoring	IT needs real-time visibility to every device and user for rapid problem resolution and performance monitoring	No difference – Users must be monitored individually, whether connected to a thick AP or thin AP
Configuration management	IT must be able to centrally define and manage all security and network policies	Thin AP architecture reduces the number of devices that must be configured separately, but management software should automate the process in either architecture.
Firmware management	IT must be able to distribute new manufacturer firmware updates to all network devices	Thin AP architecture reduces the number of devices whose software must be updated on a regular basis.
Discovery	New devices connected anywhere on the network must be automatically discovered by the management system.	No significant difference
Audit & Compliance management	Every network device must be audited continually to ensure that its configuration settings are in full compliance with policies	No significant difference – On a network with more than a handful of devices, manual audits of either controllers or intelligent APs are too labor-intensive to be feasible. Audit capabilities of the management software are the critical factor.
RF Visualization and Location Services	IT must have access to heatmaps and RF coverage maps, and must be able to determine where each user and device is located in physical space.	No difference – RF data must be gathered from every individual AP (thick or thin) and analyzed by a management system with location capabilities.
Reporting	IT needs a full set of historical trend reports to analyze network usage and performance	No difference
Alerting & Diagnostics	IT needs tools to continuously monitor the wireless network and alert appropriate individuals when potential problems are detected.	No difference
Intrusion Detection & Rogue AP Detection	IT must be able to detect any unauthorized WiFi devices connected to the network.	No difference
Multi-vendor Support	IT must be able to manage devices from multiple vendors as networks become more heterogeneous over time.	No difference

You need to carefully assess your real-world requirements to determine whether it makes more sense for your organization to use thin or thick access points. In many cases, the answer will be “both” – either because your organization has an existing, legacy WiFi network that



The true function of a wireless management system is not to restrict your options but to preserve your flexibility

must be managed or because you consciously select different technologies to meet your needs in different network or operating environments.

No matter what architectural decision you make, if your wireless network will consist of more than a handful of access points, you will need an enterprise-class wireless network management solution to deliver reliable performance and security while controlling your operating costs. The role of a wireless management system is not to dictate your network architecture, but to make your secure wireless network easy to control. Any viable wireless management solution for the enterprise should have the ability to manage both thick and thin wireless access points. Beyond that, the main questions that you should ask in selecting the right management solution are:

- Does the solution give me the flexibility I need to manage my wireless LAN today and in the future?
- Does it give me full visibility to every user and device so I know exactly what is happening and how my network is performing at all times?
- Is the solution easy to use for my entire IT staff, including network engineers, help desk and security staff?
- Does the solution make my network more secure?
- Will the solution help me control the cost of operating and supporting a new wireless network?

Meeting the Wireless Management Challenge

The AirWave Wireless Management Suite is an integrated set of software applications designed to give you a comprehensive, end-to-end management solution for your entire wireless network, regardless of architecture. The AirWave Management Suite consists of four key components:

AirWave Management Platform™ (AMP)

AMP gives you a single web-based console from which to monitor and configure your wireless network. It performs critical management tasks including device discovery, configuration management, monitoring, alerting and diagnostics, historical reporting and much more. Compared to other management products, AMP delivers an extremely easy to use interface, providing detailed real-time information on every user and device connected to the network. Unlike proprietary solutions, AMP manages both thick and thin WiFi product lines





from Cisco, Aruba Networks, ProCurve Networking by HP, Symbol, Proxim, Enterasys, Avaya, Juniper Networks, Colubris Networks, Nomadix, and many other vendors.

VisualRF™ Module

The VisualRF software module gives you a real-time map of your wireless environment, showing you accurate user and device locations, RF heatmaps, channel coverage maps, and more. Unlike other solutions, VisualRF continuously consumes real-time RF information from AMP to reassess your RF environment and provide the most accurate location information possible, without requiring a separate server or proprietary sensors.

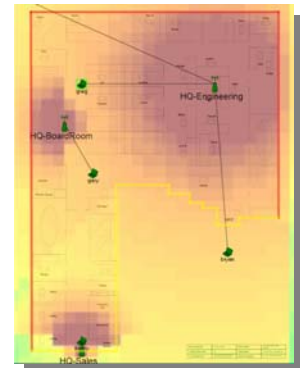


Figure 1. VisualRF Heatmap with User Location Tracking

RAPIDS™ Rogue Detection Module

The RAPIDS module uses a unique, patent-pending combination of wireless and wired network scans to alert you whenever unauthorized WiFi access points are connected to your network, either by your own users or malicious intruders. Unlike solutions that rely on wireless scanning alone, RAPIDS can detect even rogues located in remote offices thousands of miles away where you have no authorized WiFi infrastructure.

AirWave Wireless Site Plan™ (AWSP)

AWSP is an offline planning tool based on Microsoft Visio that allows you to generate an initial WiFi site plan, using any existing map, floorplan or picture as the basis for your plan. AWSP then helps you determine where your APs should be located and to predict what your resulting coverage will be. Once you have completed your plan, AWSP generates detailed installation reports and workflow documents for your installers. AWSP then exports your plan to AMP, which automatically discovers the APs when installed, configures the devices to match your plan, and updates the RF maps with real-time information in VisualRF, turning your initial plan into a living document that is constantly kept up to date.

Together, these software applications constitute the AirWave Wireless Management Suite, giving you one comprehensive solution to meet all your wireless management needs.

Providing the Flexibility You Need

Multi-architecture Networks: Managing Through Thick and Thin and Beyond

In your organization is like thousands of others, you do not have the luxury of engaging in a lengthy academic debate over the benefits of thick versus thin APs. In the real world, many organizations have to confront the reality of mixed networks with both thick and thin APs.



Many organizations today have already installed hundreds or even thousands of thick wireless access points, and are continuing to add more devices as their networks grow organically. Even if they start migrating to a thin AP architecture for most future installations, they will need to manage their legacy equipment for many years to come.

Many other organizations are intentionally installing mixed WiFi environments on an ongoing basis, using stand-alone thick APs in small remote environments like retail stores and small regional offices while using a thin AP solution in the denser campus environments. Indeed, largely because different products may be better suited for certain operating environments and customers, many leading WiFi vendors offer both thick and thin AP product lines today.

In either case, organizations with mixed architecture networks need management solutions that allow them to define security policies and control configurations across the entire network, regardless of architecture. Surprisingly, even hardware vendors who offer both thick and thin product lines sometimes cannot offer integrated management solutions, leaving their customers to choose from a series of relatively unattractive options. In contrast, AirWave software allows you to manage both thick and thin APs from the same console.

Options: Proprietary, Single-Architecture Management Solutions	Options: AirWave Wireless Management Suite
Treat your thick and thin AP installations as separate networks, managed from separate consoles – dramatically increasing training costs and complicating support.	Manage thick and thin wireless access points from the same easy-to-use web-based console, with fully integrated reporting and monitoring.
"Convert" your thick APs to thin APs (i.e., LWAPP, CAPWAP, etc.) in a complicated and potentially error-prone process – and probably losing your historical user and performance data.	<p>Multiple options include:</p> <ul style="list-style-type: none"> (a) Leaving your existing thick APs alone and managing both via AMP (b) Gradually converting your thick APs to LWAPP on a more controlled, less risky schedule <p>In either case, AirWave retains all performance and usage data, so you do not lose your entire history when you convert or replace access points.</p>
Rip out and replace your legacy infrastructure before the end of its useful life in order to have a uniform operating environment that you can manage from one console.	Extend the life of existing hardware by years, dramatically reducing equipment costs.

Integrating management of your entire infrastructure will save your organization time and money. Your help desk staff and network engineers have one single console where they can access all the information they need to quickly resolve user problems, enforce security policies, and control the network. You will not need to maintain separate management solutions and train your entire staff to use both.



AirWave customers extend the life of their existing legacy WiFi infrastructure by an average of 1.3 years

In addition to more efficient support, you will likely be able to significantly extend the useful life of your existing WiFi infrastructure by using AMP. In fact, AirWave customers report that, on average, they are able to extend the life of their WiFi hardware by 1.3 years with the AirWave Management Platform¹. NetworkWorld magazine reports that IT organizations typically expect WiFi access points and switches to last 3 years.² Increasing the lifespan of this equipment by 1.3 years could thus reduce long-term hardware costs by 40% or more.

Enterprise-grade wireless access points often cost \$400 or more even after manufacturer discounts, and can easily cost another \$100-200 to stage and install. In a mid-sized organization with 500 existing wireless access points, extending the life of this legacy equipment means that \$200,000 - \$300,000 of spending might be postponed for one or more budget years, freeing IT's time and money to address more pressing problems.

Architectural change is not an issue that organizations need to consider today and never think about again. Technical innovation in the WiFi industry continues at a blistering pace. New technologies and new architectures are inevitable, making today's 'next generation' wireless infrastructure tomorrow's legacy equipment. Intelligent organizations are recognizing that the ability to manage diverse, multi-generational wireless LANs will be the key to controlling costs and getting the most from their investment in wireless technologies on an ongoing basis. Your management software must provide the flexibility to handle this diversity, both today and in the future.

Multi-Vendor Management Ensures Adaptability

In the early days of wired networking, few organizations set out with a goal of creating vast heterogeneous network environments with equipment from multiple vendors. Yet, years later, it is virtually impossible to find a Fortune 500 organization with a true 'single-vendor' network infrastructure from end to end. Why?

One major contributor to network diversity is the acceleration of merger and acquisition activity in the corporate world. In 2005, there were more than 10,500 mergers and acquisitions in the United States alone.³ Many large corporations routinely acquire several competitors or complementary businesses every year. In the aftermath of these transactions, the CIO is responsible for integrating systems and driving down costs. A responsible CIO cannot simply hope that he will be fortunate enough to acquire only companies with an infrastructure identical to his own. Instead, a prudent CIO plans for diversity and implements systems capable of managing and controlling heterogeneous infrastructures even before the merger takes place. Because the AirWave Management Platform software controls hardware from most leading WiFi providers, it helps you effectively control and implement uniform policies across diverse network

¹ Source: AirWave Wireless Inc. Customer Survey, June 2006

² NetworkWorld, 28 November 2005.

³ FactSet MergerStat



environments. Even if you do not have a multi-vendor infrastructure today, AMP effectively provides you an insurance policy in case you inherit one tomorrow.

Another major factor leading to diversity is the tendency in very large organizations to push many project-level network purchasing decisions down to a divisional level. In leading multi-billion dollar corporations, divisions responsible for their own P&L often have their own IT and purchasing staffs, and select the technology solutions that best meet their own needs. In many cases, this means they choose products from different providers. In the past, this did not pose significant operational challenges since these divisions often functioned somewhat independently. Now, however, Sarbanes-Oxley and other regulatory requirements have made enterprise-wide configuration management and network audit C-level subjects of concern. Corporate executives need to know that security policies have been implemented consistently across all divisions, regardless of infrastructure. AMP is invaluable for these organizations, enabling them to harness a diverse infrastructure and enforce policies uniformly without replacing the underlying infrastructure itself.

Finally, because the pace of technology innovation in the networking industry is staggering, and a company whose hardware products were state-of-the-art two years ago may very well be a technology laggard today. In such a dynamic and rapidly changing market, selecting a proprietary single-vendor network management solution will likely mean forgoing innovation or accepting a more rapid hardware replacement cycle and ongoing inefficiency in managing a diverse network. The only way to ensure that you will always be able to benefit from ongoing innovation is to avoid locking yourself into a single vendor technology.

Staying Single-Vendor is No Defense

In today's rapidly-changing wireless industry, attempting to shield yourself from the complexities of heterogeneous network management by purchasing hardware only from a single manufacturer is no defense. In the WiFi industry in the 18 months from January 2005 through June 2006, there were at least:

- 3 major acquisitions of WiFi vendors⁴
- 4 major brands switching their primary OEM relationship⁵
- Multiple new OEM agreements in which one provider licensed technology from another
- Dozens of new product line introductions.

Following these changes, in some cases, the vendor implemented support for new and legacy products from a single platform, but in other cases the brand's current-generation management solution no longer has the ability to manage and support its prior hardware versions. In this tumultuous environment, there can be no guarantee that the product line you are using today will

⁴ Cisco acquired Airespace, Siemens acquired Chantry, Terabeam/YDI acquired Proxim.

⁵ Alcatel and NEC switched from Airespace to Aruba; Nortel and 3Com switched from Airespace to Trapeze



Managing Your Wireless LAN Through Thick and Thin

be supported by your vendor tomorrow. If this happens, you may be forced to purchase a new management system, replace existing hardware, or both.

Your best defense in a rapidly changing market is to select a vendor-independent management solution like the AirWave Wireless Management Suite that supports most leading vendors and multiple wireless LAN architectures.

Flexibility Means You Have Room to Grow

While it is critically important that you select management solution flexible enough to manage a diverse network infrastructure, it may be equally important that you have a solution flexible enough to manage thousands of wireless access points as your WLAN expands. Only a few organizations will see wireless traffic overtake the volume in their wired network in the next 2-3 years. However, it is certain that both the number of users and devices on your WiFi network will be significantly higher than today. While some WLAN controllers can support several hundred wireless access points, large organizations will need many thousands of APs to provide the coverage and capacity they require. Yet, the IT organization in these large organizations still must have the ability to monitor the entire network from a single console, ensure compliance to security policies, and generate network-wide reports.

With some proprietary thin AP management solutions, you cannot centralize management when multiple controllers are required. In effect, each segment of your wireless network is treated as an independent "silo" that is managed and monitored via a separate console.

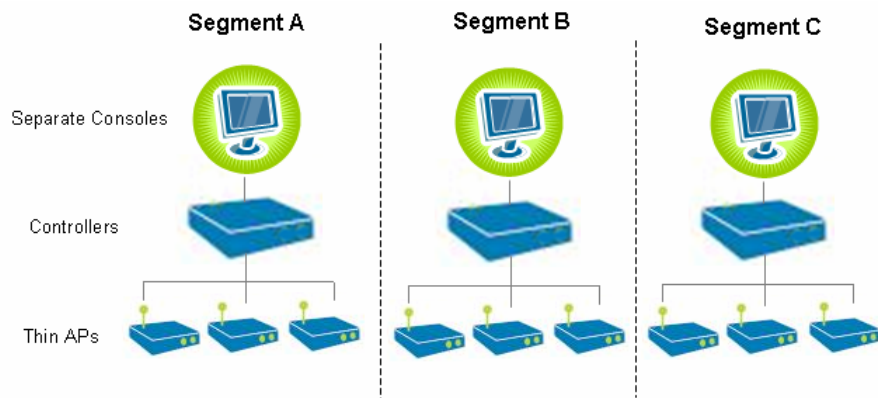


Figure 2. Managing Large Networks Via Separate Consoles

The AirWave Master Console gives you visibility to your entire WLAN, no matter how large, from a single management console. Using a distributed architecture, you can deploy the AirWave Management Platform software on as many servers (in as many different network operations centers) as required to manage a network with thousands or tens of thousands of wireless



access points.

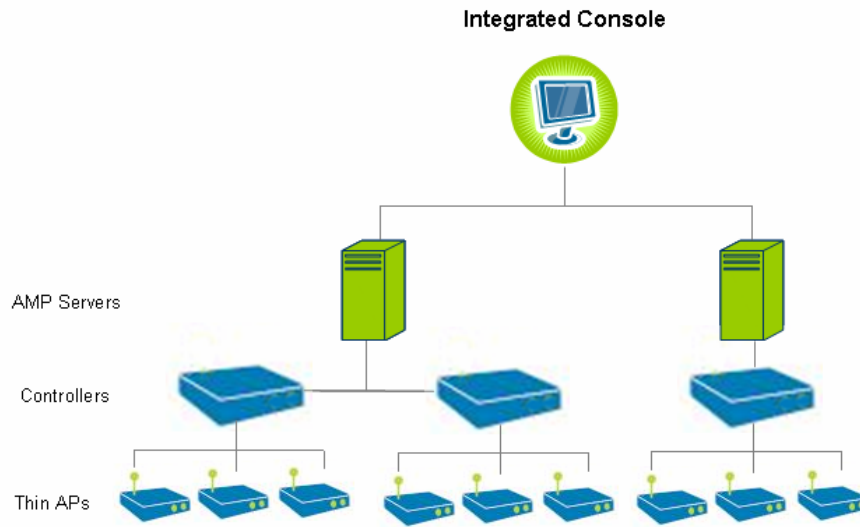


Figure 3. Integrated Management with the AirWave Master Console

The AirWave Master Console communicates with all these different servers, so you only have to look at one integrated console to see what is happening anywhere on your network.

Visibility: You Cannot Manage What You Cannot See

With thick APs or thin, visibility is the key to ensuring WLAN performance and resolving any user problems quickly. If you cannot see everything that is happening on the network – who is connected, where they are located, whether any problems are occurring – you cannot hope to deliver the levels of performance required to support mission-critical applications on a wireless network. Network visibility is not a 'nice-to-have' feature in the enterprise – it is an absolute requirement for improving performance and controlling costs. Using the AirWave Management Platform, for example, customers on average report a 35% reduction in problem resolution time and a 14% reduction in the overall incidence of user-reported problems on the wireless network.⁶ In an organization with thousands of users and hundreds of wireless access points, these savings can translate to hundreds of thousands of dollars every year.

Real-time User & Device Monitoring

The key to visibility is having ready access to real-time information on every user and device connected to the wireless network. In fact, in a recent poll of network administrators, user and device monitoring was the single most important feature a wireless management system can provide.

AirWave customers report an average 35% reduction in wireless problem resolution time and a 14% reduction in the incidence of user reported wireless problems.

⁶ AirWave Customer Survey, June 2006



Managing Your Wireless LAN Through Thick and Thin

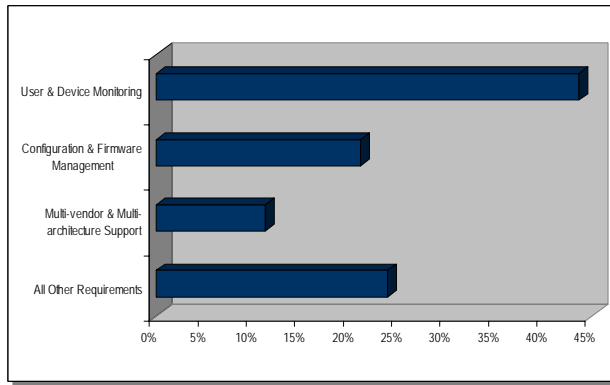


Figure 4. Top Wireless Management Priority (AirWave Customer Survey, June 2006)

Many proprietary management systems rely heavily on reports for user data, requiring specific jobs to be scheduled and run when user data is needed. For a service-oriented IT department, this is not good enough. When users call to report that the network is slow or that they cannot connect, your Help Desk needs instant access to real-time information while the user is on the phone. With the AirWave Management Platform, real-time monitoring views of any user or device are only a few mouse-clicks away at any time.

With AMP, you can instantly call up a detailed monitoring view for any access point or device on the network, seeing who is connected to the device, which radios they are using, how much bandwidth is being consumed, examining any alerts or errors related to the device, and much more. Network engineers can see real-time graphs showing RF statistics (“802.11 counters”) to help them diagnose wireless problems – and can even see charts comparing current error levels to those experienced over the past hours, days, weeks, months, and years to more accurately determine the source of the problem.

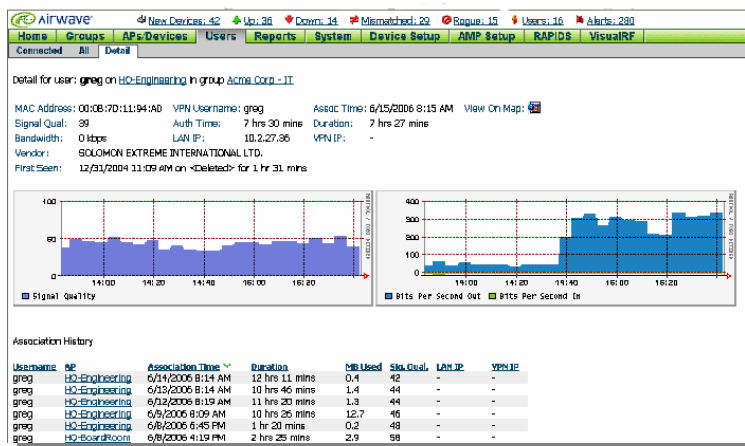


Figure 5. User Monitoring View with Signal Strength, Bandwidth, & Roaming History

They can even drill down to individual user views for any user on the network, seeing real-time graphs showing changes in the user’s signal strength and bandwidth utilization over time.

Historical Trend Reporting

The writer George Santayana famously observed, "Those who cannot learn from history are doomed to repeat it." In supporting your wireless network, detailed historical reports are the key to avoiding errors and improving network performance. Network engineers and planners need accurate usage statistics to determine where problems are occurring and whether capacity is in danger of being exceeded. As more organizations implement wireless VOIP and other applications with stringent performance requirements, planners must be able to track not just overall network usage, but QoS statistics and other data on a VLAN-by-VLAN basis.

Because usage patterns may change radically by time of day or year, historical trend reports must date back not just several weeks, but for months and years. In a retail distribution center, for example, network engineers need previous-year data to project how wireless network load might increase during the holiday period. And for a K-12 network administrator, network usage statistics from July and August are useless in planning for the upcoming school year; they need information dating back to the previous academic year. For almost any organization, retaining at least twelve months usage data for trend reports is essential for network planning purposes.

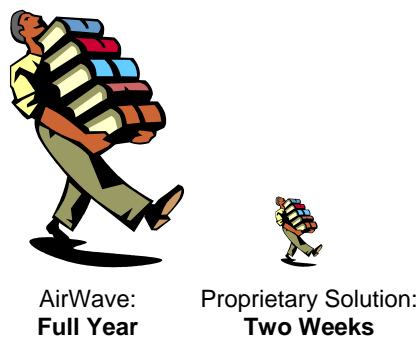


Figure 6. User History Retained

The AirWave Management Platform efficiently stores all key usage data for at least twelve months, and up to two years. All reports are easily exportable via XHTML, so the information can be retained and analyzed with other applications as well.

While this type of historical data is obviously needed for planning purposes, it is equally essential in accurately and quickly diagnosing real-time user problems. If a user calls to complain that the wireless network is slow on a given day, the help desk staff must have ready access to historical information: Is the signal strength the user is receiving any different than what he or she normally receives? Is the user connected to the same AP and the same location as usual? Has there been a recent increase in RF errors in that area? Without historical information, the help desk and network engineers have no context within which to



analyze the problem and will end up exploring many dead-end paths in trying to determine the root cause of any problem. With historical data, you can quickly zero in on and address the true source of the problem.

Location Information and RF Monitoring

Unlike wired network users, wireless users can be highly mobile. This dramatically increases the complexity of supporting wireless users. Where they connect to the network is constantly changing, and RF conditions in that environment today may be radically different than they were yesterday. This is particularly true in urban and multi-tenant environments, where your neighbors' overlapping wireless networks can dramatically impact the performance and range of your own network.

To manage a wireless network effectively, you must have up-to-date RF maps to help you understand the wireless environment and must be able to determine where each user and device is located. Yet, surprisingly few organizations have this information at their fingertips today. In many cases, RF site surveys conducted months or years ago sit unused in a drawer gathering dust even as RF conditions change and evolve. Often, the IT organization simply could not afford the expense of installing and using dedicated RF sensors to scan and map the RF environment on an ongoing basis. As a result, the IT staff is essentially flying blind, unable to see what is happening in their airspace and unable to resolve user problems as they occur.

AirWave's VisualRF module ensures that you always have an up-to-date RF map with device location information, without proprietary sensors or expensive additional servers. Using the offline AirWave Wireless Site Plan software or online VisualRF interface, your planners and network installers can quickly import any existing drawing or floorplan and use it as the basis for an initial RF plan. VisualRF then updates this plan with real-time RF information from your existing wireless access points to generate:

- Heatmaps (showing the signal strength available at all locations on the map);
- RF channel maps (indicating channel settings of APs and identifying potential areas of interference);
- Location maps (showing where users and devices are located in physical space).

The VisualRF location module is especially accurate because (when supported by the WiFi hardware) it incorporates data from both clients associated to a particular access point as well

Strengths of the Visual RF Module

- Uses data from existing APs and controllers rather than requiring dedicated sensors or APs running in sensor mode.
- Fully integrated with AirWave Management Platform on a single server instead of requiring a separate server for location services.
- Uses RF data from unassociated clients for maximum location accuracy
- Frequently updates RF attenuation grids for accuracy instead of relying on static or infrequently updated RF information.
- Accurate location information and RF maps even in a multi-vendor environment

as unassociated clients connected to other access points. Relying only on associated client data limits the number of data points that can be used to locate the user. Incorporating data from unassociated clients greatly increases the number of data points available for location triangulation.

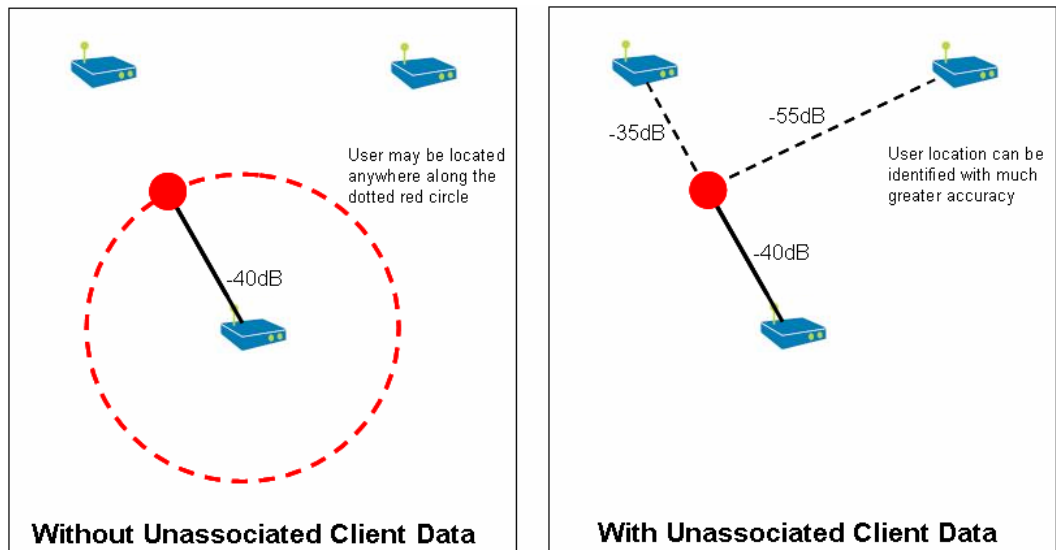


Figure 7. Using Unassociated Client Data to Increase Location Accuracy

Unlike some location solutions, VisualRF frequently recalculates its RF attenuation grid (used to calculate heatmaps and locate devices), always using the most up-to-date information available to ensure maximum accuracy. And, as a vendor-independent solution, VisualRF gathers and displays data from leading access points and controllers, ensuring an accurate RF rendering even in complex, multi-vendor environments.

Usability for Your Entire IT Staff

At some point in his career, every IT manager discovers an expensive software package sitting on the shelf gathering dust because it turned out to be too difficult to install and use. A good network management product must be designed for ease of use, not just for an experienced network engineer but also for the help desk support staff, auditors, managers, and the dozens of other IT employees who will need to use the system. If the system is not simple and intuitive, all these other employees will have to rely on the network engineers to gather information for them and perform even the most basic tasks on the network. Even worse, when IT systems are not usable, those network engineers may need to invest their own time and effort in building and supporting custom scripts and applications, often at great ongoing cost to the organization.

From both a financial and operational perspective, it is imperative that network engineers not become the bottleneck in supporting the wireless network. In a typical IT organization, the help



desk staff is charged with responding to user issues and client problems, while only network-related issues are to be escalated to network engineering.

According to NetworkWorld magazine's annual IT salary survey, network analysts and administrators earn, on average, 25-50% more than help desk support staff.

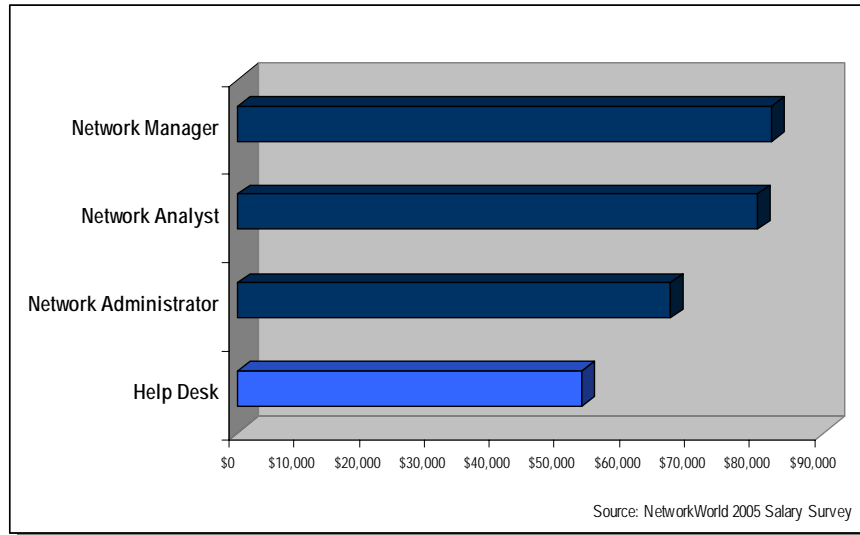


Figure 8. Average Annual Salaries of IT Staff Members

Every time an issue that could be handled by the help desk is escalated to a network analyst instead, your organization is paying 25-50% too much. Even in moderate-sized organizations, the excessive reliance on network engineers to resolve wireless problems can easily amount to tens of thousands of dollars per year in salary and overtime.

Even worse, when network engineers have to spend their time addressing end-user issues and other wireless problems, they cannot address more critical network and security-related IT functions. The 'opportunity cost' of using network engineers to support wireless LAN users can amount to hundreds of thousands of dollars in lost efficiency and sub-optimal security practices.

Help Desk Functionality

AirWave's web-based user interface has many features designed specifically to make the software easy for the help desk staff to use. In a recent survey of customers who had evaluated both AirWave software and a leading vendor-provided 'thin AP' management system, 100% of the survey respondents agreed that the AirWave software was significantly easier to use.⁷

Quick UI links help users navigate the system to get the information they need with just a few mouse-clicks. When the help desk staff member receives a wireless user support call, AirWave's

⁷ AirWave Customer Survey, June 2006



sophisticated user search function allows him or her to immediately locate the user on the network by username (rather than solely by MAC address or IP address – which most users are unlikely to be able to provide over the phone).

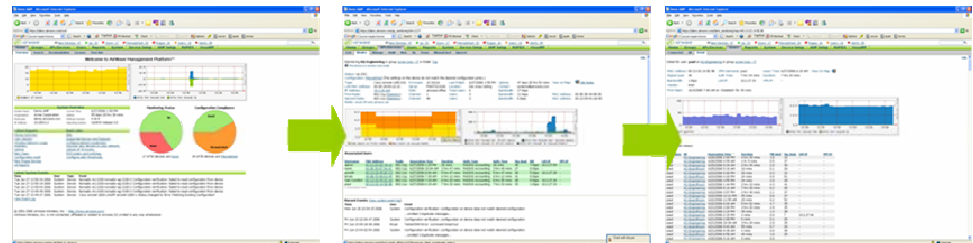


Figure 9. Drilling Down from a Network View → AP View → User View

The Help Desk can determine exactly which access point the user is connected to, call up real-time and historical data for the user and device, determine how many other users are connected through the same AP, assess usage conditions, and determine whether any other users are experiencing similar problems.

Role-based Views

For your IT department, seeing too much information can be as big a problem as not seeing enough. In large organizations with hundreds of wireless access points and thousands of users, there can easily be tens of thousands of wireless 'events' every day, creating an enormous amount of data for your IT staff to wade through when investigating issues. In large organizations, there is typically no single person responsible for the entire wireless network. Instead, the work of supporting the network is intelligently sub-divided among many different individuals and groups: The help desk supports end users, network engineers are responsible for overall network performance and uptime, the security staff handles audits, and so on. Responsibilities may be further sub-divided by geographic region (i.e., one group supports North American operations while another supports EMEA), division (i.e., retail store locations versus corporate headquarters), or other logical grouping.

A truly usable management system allows views and privileges to be individually tailored so that every user sees the information needed to do his job, without being overwhelmed by information not relevant to his responsibilities. The AirWave Management Platform allows you to assign management privileges and customize views that make sense for your organization. A Help Desk user may be given 'view-only' monitoring privileges for a segment of the network (so he can see real-time views, historical reports and alerts related to users and devices in that network segment), but may not see monitoring information from areas outside his scope of authority.



Enforcing Network Security Across the Entire Network

Network and data security have always been top priorities for CIOs in Fortune 500 organizations. Now, however, with the compliance and oversight obligations imposed by Sarbanes-Oxley, HIPAA, Payment Card Industry (PCI) standards and other mandatory programs, wireless network security is an executive-level concern in any organization.

Over the past several years, networking industry press and other experts have extensively debated the best methods of wireless encryption, authentication, and access control (WEP vs. WPA vs. WPA2, etc.). While this debate has yielded significant improvements in wireless security practices, these experts have not focused enough attention on network management's role as the foundation of any successful security policy. You must always assess risks and costs to determine the security policies that best meet your organization's needs – but no matter what choices you make, you need an effective network management system to implement and enforce those policies uniformly.

Automated Compliance Management versus Manual Solutions

The first, and perhaps most important, security function of a wireless network management system is to enforce configuration policies uniformly across all wireless access points and controllers, and to continuously audit the wireless infrastructure to ensure that those policies remain in effect at all times.

The Gartner Group has estimated that 90% of wireless security incidents will be caused by misconfigured devices and infrastructure. If the organizations' policy is that WPA should be used for secure wireless access, then every access point, switch, and controller on the network must be configured to support that policy. If WPA gets disabled on any AP, that device can become an open window through which intruders can gain access to the organizations' secure network resources. Misconfigured access points and controllers can be extremely difficult to locate because they may continue to function normally and show no signs of problems until it is too late.

Often these configuration errors are made when the wireless device is first installed. However, it is not enough to correct installation and provisioning processes alone. Many things can cause a device to become misconfigured during the course of normal network operation: human error, failure to apply firmware updates uniformly across the network, devices that were 'down' when configuration changes were applied but subsequently resume functioning, devices that

Gartner Group estimates that 90% of wireless security incidents will result from misconfigured devices and infrastructure.

What is Automated Wireless Compliance Management?

- Continuous configuration audit
- Network-wide compliance scans
- Automated alerts for violations
- Side-by-side detailed reports for any misconfigured device
- Auto-repair of misconfigured devices without human intervention



reset when re-booting or updating, etc. In a survey of AirWave customers, including many with both thick and thin APs, customers reported that on average they discovered a staggering 32% of their wireless devices were misconfigured before using the AirWave software.⁸

Responsible organizations concerned about security need to implement processes to ensure that every wireless device is audited for compliance with configuration policies at least once per day, if not more frequently. Configuration violations must be repaired as soon as they occur.

Whether an organization has thousands of stand-alone wireless APs or several dozen controllers and switches with thin APs, manual audits are not an acceptable solution: (1) they are too time-consuming to be conducted regularly, and (2) manual processes are themselves subject to human error.

Some proprietary wireless network management solutions from hardware vendors offer only a semi-automated auditing process in which a detailed configuration reports showing the current device configuration and the corresponding policy settings can be generated on a device-by-device basis. Again, however, for any organization with more than a handful of configurable wireless devices, this is not good enough. Network auditors still need to initiate and comb through these reports, implementing changes manually. Even worse, if the organization has multiple controllers with separate management consoles, the auditors may have to repeat the entire process on a console-by-console basis.

In contrast with such time-consuming manual processes, AirWave offers a more secure solution designed to ensure that misconfigured devices do not lead to security breaches: **Automated Wireless Compliance Management**. At a specified interval, the AirWave Management Platform compares the current configuration of every device on your wireless network with the policies you have specified. When any variance is detected, AMP generates an alert and emails you a link to a detailed side-by-side onscreen report showing specifically which settings are out of compliance.

Using AMP's web-based user interface, you can immediately correct the device configuration to bring it back into compliance right away. You can even instruct AMP to automatically 'repair' configuration violations as soon as they are detected, eliminating the need for human intervention and ensuring that your network is free from configuration errors at all times. For large organizations that distribute the

Customers discovered that an average of 32% of their wireless devices were misconfigured before using AMP

AP Settings		
	Device Config	Desired Config
Administrative Status	Enabled	
Gateway	10.51.0.1	
LAN IP AP Uses	10.51.1.42	
Mode	Local	
Name	aironet-1030-3	airespace-1250-2
Netmask	255.255.0.0	
Primary Controller	Cisco-4402-1	
Secondary Controller	(empty string)	Airespace-4012-1
Tertiary Controller	(empty string)	Airespace-4012-2
Use DHCP	Yes	
System Properties		
	Device Config	
Description	Cisco Controller	
Location	default_location	
ObjectID	.1.3.6.1.4.1.14179.1.1.4.3	
Uptime	14 hrs 43 mins	
802.11g Radio		
	Device Config	Desired Config
Allow Automatic Channel Selection	No	
Antenna Diversity	Enabled	Side A
Antenna Type	Internal	
Automatic Transmit Power	Enabled	Disabled

Figure 10. AirWave Side-by-Side Device Compliance Report

⁸ AirWave Customer Survey, June 2006



management software across multiple servers for efficiency, the AirWave Master Console provides a single report showing all misconfigured devices, no matter where they are located on the network.

Rogue access point detection

While you must always take steps to ensure that none of your own wireless devices become misconfigured, you must also have a strategy to detect any unauthorized 'rogue' wireless access points on your network. Indeed, the rapid proliferation of WiFi technology in the consumer market has made rogue detection a paramount priority in any IT organization. Rogue access points are by no means rare or uncommon. In fact, AirWave customers using the RAPIDS rogue detection software report that, on average, they discover 67 rogue devices on their network.⁹

Customers discovered an average of 67 rogue devices on their network when implementing RAPIDS

In the past, few of your employees probably had the knowledge, money, or incentive to bring their own routers to the office and connect them to your Ethernet network. Now, however, any employee can easily bring the same low-end WiFi access point he uses at home into the office. In fact, the vast majority of rogue access points today are installed not by intruders but by employees seeking wireless access in the workplace. Since these employees rarely have the knowledge or resources to secure the rogue AP, their unprotected rogue devices offer intruders a direct path onto the enterprise network.

In a large organization, the most likely place to find rogue APs is in a facility that does not yet have a readily available WiFi network for employee use – especially in small remote facilities far from the watchful eye of the IT security team.

Many proprietary wireless management solutions use existing thick or thin WiFi access points (or APs operating in 'dedicated sensor' mode) to scan the RF spectrum looking for other unknown access points within range. Since any rogue AP that can be used by an intruder to access your network must emit RF signal, this is a highly reliable technique for detecting and locating rogues. Where existing APs are in place, AirWave's RAPIDS software uses this RF data to detect and triangulate the physical location of the rogue device.

However, relying exclusively on RF-based rogue detection alone is rarely a safe policy for a large organization, for the simple reason that very few have true enterprise-wide, wall-to-wall wireless coverage (via APs or sensors) today. The largest 1,000 corporations in the U.S.

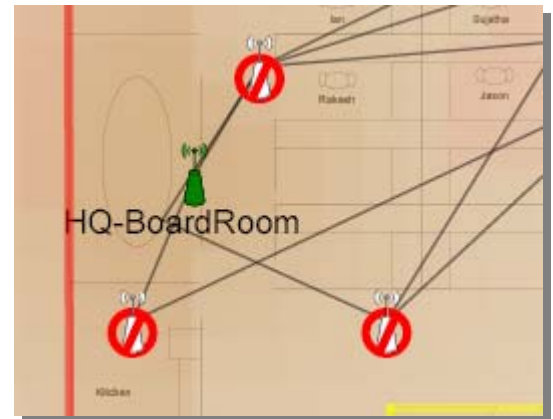


Figure 11. Locating Rogue APs with RF Data

⁹ AirWave Customer Survey, June 2006



average roughly 600 separate facilities.¹⁰ It will be many years before most of these organizations have wireless in every one of these facilities – and these areas without wireless coverage are the most vulnerable to rogues. Wireless rogue detection techniques are thus least effective in the spots where rogues are most likely to be found: remote locations where there is no authorized wireless network.

AirWave resolves this conundrum by combining wireless detection techniques with scans of the wired network infrastructure. Using AirWave's database of more than 10,000 AP 'signatures', RAPIDS communicates with your existing routers and switches, assessing every network device and assigning it a score reflecting the likelihood that it is an unauthorized rogue AP. When likely rogues are detected, AMP sends you a high priority alert containing all the known information (from wired and wireless sources alike) about the device, including port information enabling you to find the device on your wired network. RAPIDS can also conduct more advanced wireline interrogation to reduce false positive results, examining OS data and other information to eliminate devices that are unlikely to be rogues so you and your colleagues do not waste your time pursuing false leads.

By combining wired and wireless techniques, AirWave provides a unique and affordable solution for detecting and removing rogue access points from your network before intruders find them and use them to breach your network.

Role-based Administrative Access

While a good network management solution provides the solid foundation for your entire wireless security strategy, a network management solution with a poorly designed 'one-size-fits-all' administrative access system can be your worst enemy.

'One-size' management solutions give all administrative users identical management privileges or make only rudimentary distinctions between different classes of users. These solutions are typically appropriate only for very small wireless networks, in which one member of the IT staff has primary responsibility for supporting the WLAN and wireless users.

In contrast, 'responsibility-based' access solutions, like the AirWave Management Platform, assign specific privileges and levels of management control based on the role of each individual in your organization.

When large, diverse IT organizations rely on one-size-fits-all management solutions, they pay a high price in security and performance. Good security policy is built on the principle that every user should have access only to network information that he or she truly needs in order to do his or her job. Many configuration errors and security violations are caused when IT employees unwittingly use management solutions to make changes they are not authorized or qualified to make. At best, these unauthorized actions can cause minor performance

¹⁰ U.S. Census Bureau



problems. At worst, they can invalidate security policies and expose an entire network to attack.

The AirWave Management Platform addresses this problem by giving you the ability to define the role and privileges for each user of the management system, with a unique user identifier and password to ensure accountability.

For example, help desk users may require monitoring information and historical reports, but typically are not permitted to change policies or the configuration of any network device. Security

Type of User	User & Device Monitoring	Compliance Monitoring	Configuration Management
Help Desk	◆		
Security Auditor	◆	◆	
Network Engineer	◆	◆	◆

Figure 12. Management Responsibilities in a Typical Organization

auditors should have access to audit reports, but rarely require configuration privileges or the ability to view community strings. And even a network engineer responsible for operating a wireless LAN in North America often should not have any visibility or control over the wireless network in other parts of the world.

AirWave allows you to define the level of access specifically for each group or individual, and integrates with systems like TACACS+ to apply existing access policies to your wireless network.

Results: WiFi ROI

In the final measure, whether you use thick APs or thin, any wireless network management system is an investment. Your responsibility is to determine what management solution will provide the best return on that investment: in lower operating costs, superior performance, and improved security. Proprietary management solutions developed by individual hardware vendors rarely provide the full range of functionality required by enterprises and other large organizations.

Hundreds of IT departments around the world, using thick access points, thin access points, and a combination of both, have selected the AirWave Wireless Management Suite over narrow, proprietary solutions because of its superior WiFi ROI:

- Significantly lower operating costs by reducing in the number of wireless-related incidents and more rapid problem resolution
- Improved network performance
- Integration of diverse wireless network infrastructures and the elimination of multiple separate management consoles.

94% of AirWave customers will achieve a positive return on investment within 2 years



Managing Your Wireless LAN Through Thick and Thin

- Shifting more of the burden of WLAN management from network engineers to the help desk
- Elimination of misconfigured devices and rogue access points

Assessing these factors, more than 70% of AirWave customers report that the AirWave software saved their organization from having to add at least one additional full-time employee to support their wireless networks. Even more impressive, 94% of AirWave customers report that they have achieved or will achieve a positive return on their investment in AirWave software within 2 years, and more than 55% will do so in 12 months or less.¹¹

AirWave Wireless, Inc.

1700 South El Camino Real
Suite 500
San Mateo, CA 94041

+1.650.286.6100

+1.650.286.6101 (fax)

info@airwave.com

www.airwave.com

© 2006, AirWave Wireless, Inc. All rights reserved. AirWave, the AirWave logo, AMP, AirWave Management Platform, VisualRF and RAPIDS are trademarks of AirWave Wireless, Inc. Other company and product names used herein are the trademarks of their respective owners.

WP - Thin - 0606

¹¹ AirWave Customer Survey, June 2006.



Appendix: 12 Simple Questions to Ask Your Hardware Vendor About Wireless Network Management

Many organizations using thick or thin APs will at least evaluate their primary hardware vendor's proprietary management solution before implementing the AirWave Wireless Management Suite. Before adopting a proprietary management solution, you should ask your hardware vendor to respond to the following 12 questions:

Question	AirWave	Hardware Vendor
1. Does the management solution support both thick and thin access points?	Yes	
2. Can the management solution support other vendors' hardware if that becomes necessary in the future?	Yes	
3. Does the management solution provide real-time monitoring views for every user and device on the network?	Yes	
4. Do the solution's historical reports date back twelve months or more?	Yes	
5. Does the solution provide side-by-side onscreen audit reports comparing current device configuration to policy?	Yes	
6. Can the solution automatically repair misconfigured devices?	Yes	
7. Does the solution detect rogue APs that are not in range of wireless access points or sensors?	Yes	
8. Does the solution allow administrative privileges to be defined by role and by network segment?	Yes	
9. Can the solution provide a single console from which to monitor 5,000+ wireless access points?	Yes	
10. Does the solution include integrated location services or is a separate server required?	Yes	
11. Are all users and device locations calculated and recalibrated every ten minutes?	Yes	
12. Does the solution have real-time monitoring screens specifically designed for help desk users?	Yes	