



Unlocking the Value of Your Cisco WLAN: Best of Breed Wireless Management for Cisco Customers

Overview:

AirWave – The Key to Unlocking the Value of Your Cisco Wireless LAN

Cisco is the largest provider of Wi-Fi hardware to global enterprises and other large organizations, with an extensive product line encompassing 'intelligent' Aironet wireless access points, 'thin' Airespace access points and switches, and the CiscoWorks WLSE element manager.

Why, then, have so many leading organizations like the United States Joint Forces Command, Newell Rubbermaid, Vanderbilt University, and the University of Wisconsin at Madison turned to the AirWave Management Platform™ to operate their 'all-Cisco' wireless networks? In fact, more than 50% of AirWave's customers use AMP to manage Cisco networks.

Many of these organizations were not getting the value they expected out of the high-end Cisco Wi-Fi infrastructure that they spent tens of thousands of dollars to purchase and deploy. While end users loved the mobility enabled by the wireless network, operating the network was costly and time-consuming for the IT department.

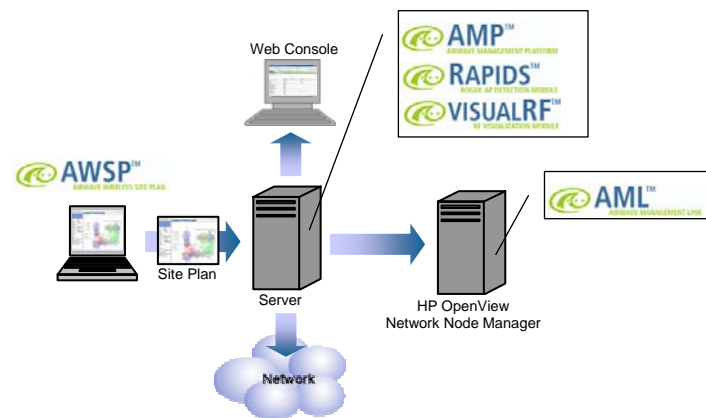
These organizations turn to AMP for the same reason they use products like HP OpenView to operate their traditional wired LANs: *to unlock the value of their investment in Cisco infrastructure*. Operating a network is a complex mission, involving the entire IT staff and requiring much more than simple configuration management tools. Instead, IT needs **comprehensive wireless network operations solutions** that provide real-time monitoring, intelligent diagnostics and alarms, reporting, fault management and Help Desk functionality, and much more.

By using AirWave's comprehensive software solutions to operate your Cisco wireless network, you will:

- Reduce the cost of operating your wireless network
- Enhance wireless network security
- Maintain flexibility and ensure scalability as your network grows

What is AirWave?

AirWave Wireless develops complete network operations software for managing the entire life-cycle of wireless networks, from the design of the initial site plan all the way through the ongoing monitoring of global WLANs with thousands of wireless access points and end-users. The AirWave product line includes:



Sample AirWave Network Diagram



The **AirWave Wireless Site Plan™ (AWSP)** is a simple, easy-to-use Microsoft Visio-based software application that helps network engineers design a graphical RF site plan. With AWSP, network engineers can ensure that the WLAN provides the coverage they need while minimizing RF interference. Once the site design is finalized in AWSP, network engineers simply upload the design to the AirWave Management Platform, which automatically configures the wireless network infrastructure to match the plan.



AirWave's flagship **AirWave Management Platform™ (AMP)** is a 100% software solution that installs on standard PC server hardware, typically in one or more Network Operations Centers (NOCs). The AMP software has a web-based UI that gives users a single point of intelligent control for remotely monitoring and configuring multi-vendor wireless access points and other network devices. The AMP software offers device discovery, centralized policy definition, automated configuration management and audit, firmware distribution, real-time monitoring, intelligent diagnostics, and reporting. AMP supports hardware from leading enterprise-grade vendors, including Avaya, Cisco (Aironet and Airespace), Colubris, Enterasys, Funkwerk, HP ProCurve, Intel, LANCOM, Nomadix, Proxim, Symbol, and others.

AMP includes an efficient, high-speed data collector that gathers granular, real-time data from every wireless device and user connected to the network. This data is continuously monitored and analyzed by AMP's sophisticated analytical engine to alert IT whenever problems may impact wireless network users. Depending on the nature of the problem, AMP may automatically implement corrective actions or help network administrators remotely reconfigure the network as required.



AMP's new **visualRF™** module provides real-time graphical reports on key aspects of WLAN performance. With visualRF, network administrators can view an up-to-date coverage map of any facility in their wireless network, for use in trouble-shooting or planning. VisualRF also provides graphical depictions of each wireless user's physical location on the network and generates visual reports identifying the location of potential rogue access points. (NOTE: visualRF is currently available in beta version, and will be generally available with the AMP 4.0 release.)



The **RAPIDS™ Rogue AP Detection Module** is a server-side software application that automatically detects and locates unauthorized access points through a combination of RF scanning and wireline "fingerprinting." RAPIDS uses authorized APs to scan the RF airspace for any rogue devices. It also scans the wired network to determine whether any unknown APs are connected outside the range of the authorized access points.

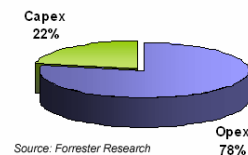


The **AirWave Management Link™ (AML)** is a Java application that facilitates integration and communication between the AirWave Management Platform and other network management solutions (such as HP OpenView Network Node Manager), enabling users to monitor and manage the wireless and wired networks as one.

How Does AirWave Reduce the Cost of Operating a Cisco Wireless Network?

Forrester Research calculates that the cost of operating a WLAN and supporting wireless users for a single year can cost organizations almost four times as much as the Wi-Fi hardware itself. As Wi-Fi hardware prices continue to fall, this ratio will only grow larger in the future. The implication of this is clear: *if you want to control costs as your wireless network grows, you need a management solution that will help you drive down operating expenses.* The easy-to-use AMP software is designed exactly for this purpose. As a result, even AirWave customers who have already purchased the WLSE appliance report that they achieve a positive Return on Investment (ROI) on the AirWave software within 6-12 months.

WLANs: Operational vs. Capital Costs



Faster Planning and Provisioning of Your Cisco WLAN

The AirWave Wireless Site Plan (AWSP) RF planning software is based on Microsoft Visio, a tool that almost every network engineer already uses on a regular basis. This allows most engineers to start using AWSP within minutes, without extensive training. Instead of having to create a new site map for each location, they can simply import whatever physical drawings already exist: CAD drawings, Visio diagrams, JPEG files of any size. Using AWSP's drag-and-drop interface, they then place their Cisco APs in the approximate physical position on the drawing, specify channel settings and other configuration parameters, and publish the plan to AMP. When AMP discovers the specified Cisco APs, it automatically configures them to match the plan, eliminating time-consuming manual configuration and human errors. With AWSP, the site planning process for an entire building can be completed in just a few minutes.

Using AMP's IOS Templates to Eliminate Configuration-related Problems

By the time they install AMP, Cisco customers often have several hundred or thousands of IOS-based access points. While these customers have usually tried to be diligent in maintaining uniform configurations (including consistent firmware versions) on all these complex devices, it is not uncommon for 30% or more of the actual device configurations to be out of compliance with the policy or to be running older firmware.

This variability in configuration parameters may be caused by: human error; differing interpretations of security policies by staff members in different locations; undetected failures in configuration or firmware updates; the inability to prevent unauthorized users from making configuration changes; the necessity of using multiple independent WLSE appliances on segments of large networks; undiscovered and unmanaged access points on the network; or many other factors.

Whatever the cause, these configuration violations are a common source of network problems and result in hours of work when network engineers have to engage in trouble-shooting activities to detect and repair them.

AMP helps eliminate these problems by providing a very simple IOS ConfigurationTemplate Tool that allows you to select a correctly configured IOS access point to serve as a configuration 'model' for other APs. AMP imports the configuration file from that device, parses it to determine which settings must be AP-specific (such as RF channel setting, transmission power, etc.) and which settings can be used as a template for other APs. Once the template is defined, you specify which APs on your network should be configured to match the template. AMP then determines what changes need to be made to implement the policy on each AP. After giving you a final opportunity to review and approve the changes, AMP automatically updates the configurations of all the APs to match the template and verifies that all updates were successful.

By providing a clean 'baseline' configuration across your entire network, numerous problems are eliminated and it becomes much easier to maintain uniform configurations on an ongoing basis.

Reduction in IT Training Time & Costs

The award-winning AirWave software has a very intuitive web-based UI that usually takes less than four hours of training to master. As your wireless LAN grows to encompass thousands of access points and users, you will need to train more and more members of your IT staff to use your WLAN management tools. If these tools are not intuitive, training costs will skyrocket, routine management tasks will take longer to perform or, even worse, the tools will not be used at all. This was one of the most important reasons the United States Joint Forces Command selected the AirWave Management Platform to manage their Cisco network:

"Most recently, the [U.S. Joint Forces Command] layered on AirWave centralized configuration and management software to help scale access point deployment. This move happened after attempting to automate access point setup with Cisco's Wireless LAN Solution Engine (WLSE) for two months and finding it "not intuitive," says Derek Krein, wireless engineer." (NetworkWorld)

Involving the Entire IT Staff: A Management Solution that Understands Your Organization Structure

IT organizations control operating costs on their wired LANs through a division of labor among the staff: Highly skilled network engineers focus on network design and policy, while Help Desk staff members handle routine matters and most end-user problems. If your WLAN management tool is so complex and difficult to use that only your network engineers can understand it, these network engineers are forced to handle even the most routine and straight-forward wireless network issues. As a result, network engineers become a bottleneck in problem resolution and cannot focus enough of their time on other, more pressing matters. Network support costs escalate because expensive network engineering resources are being used for tasks (report generation, end-user support calls, etc.) that could, and should, be handled by others.

In 2005, an average Network Manager will earn \$76K. Help Desk/Tech Support Staff will earn \$48K. Every hour of work that can be shifted to the Help Desk saves the organization ~\$20.
(Source: NetworkWorld, July 25,2005).

The easy-to-use AMP software allows you to apply the same cost-saving division of labor on your wireless LAN that you do to the rest of your network. With its specially designed Help Desk views, AMP puts all the information the Help Desk staff needs to resolve common user problems at their fingertips. AMP even allows you to specify exactly what level of access your Help Desk specialists should have: should they be able to change device configurations or simply have 'read-only' access to monitoring information? Should a specialist on a campus in San Francisco have access to data on all network devices or should his views be limited to that campus only?

By shifting responsibility for end user issues back to the Help Desk, you will not only save money and free your network engineers for other tasks, but you will also have more scalable processes that can be sustained even as your WLAN grows.

Reduction in Problem Resolution Time

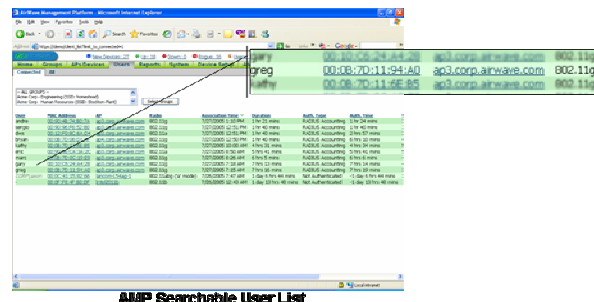
Even as AMP allows you to shift support responsibilities back to the Help Desk, it also reduces the time it takes to resolve common problems by making real-time information readily available.

“Hewlett Packard reduced average WLAN trouble ticket resolution time by 75% with the AirWave Management Platform.” (Network Magazine)

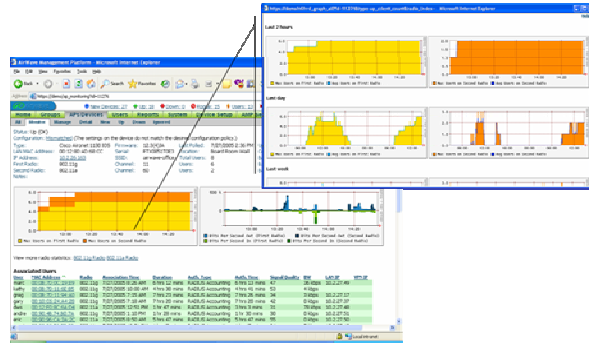
With AMP, when a user calls to report an issue, the Help Desk specialist can quickly search for the user by his username, determine which AP he or she is connected to, examine real-time performance statistics, view an RF map of the surrounding area, and even drill-down to an individual user view showing signal strength, bandwidth utilization, and a complete roaming history. With Cisco's WLSE, this information might require a job to be scheduled or reports to be generated by a network engineer. With AMP, this information is instantly available, enabling more accurate trouble-shooting and faster problem resolution.

Typical Help Desk Problem Resolution Scenario with AMP: User Calls the Help Desk to Report that the Wireless Network is 'Slow'

Step One: Locate the User on the Wireless Network (by Username)

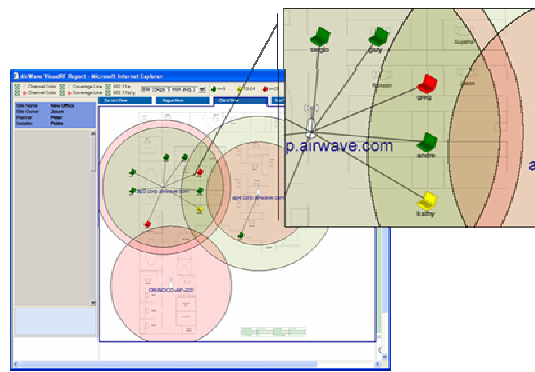


Step Two: Examine Real-time & Historical AP Usage & RF Statistics for Anomalies



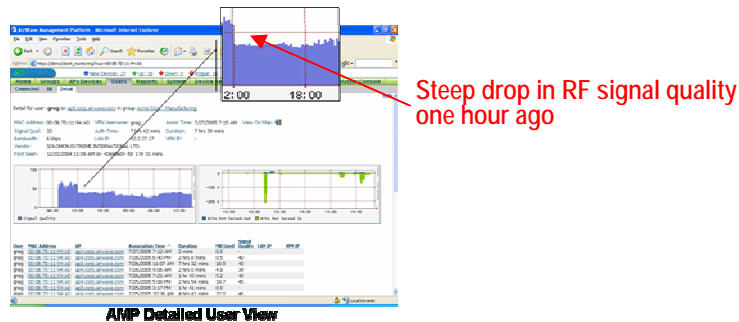
Real-time AP Monitoring Screen

Step Three: Toggle to visualRF View to Understand the Surrounding RF Environment



AMP visualRF View

Step Four: Drill Down to a Detailed User View to Assess Signal Strength, Bandwidth Use, etc.



AMP Detailed User View

Step Five: Use AMP to Increase AP Transmission Power to Provide a Stronger Signal.

With AMP, this entire trouble-shooting sequence takes two minutes or less. Real-time monitoring with AMP means that problems can be resolved in real-time as well. As a result, end user satisfaction improves even as support costs fall.

How Does AirWave Make My Cisco Wireless Network More Secure?

While reducing support costs is vitally important, every survey or study indicates that security is still the #1 concern of CIOs and IT executives related to wireless networks. Network security is always a paramount concern, but the attention being paid to Wi-Fi networks by Sarbanes-Oxley, HIPAA, Visa and other auditors makes WLAN security a topic of critical importance for the IT staff. AirWave software has many features that help ensure that your Cisco wireless network is as secure as it possibly can be.

*Automated Configuration Audit:
Automatically Eliminate the
Most Common Cause of
Network Breaches*

The first step toward securing your Cisco wireless network is to define your security policies:

- What method will you use to authenticate users on the network (WPA, WEP, wireless gateways, etc.)?
- What data encryption will be required?
- Will the same policies apply to all users (employees vs. guest) or will you segregate different classes of users on different VLANs and apply different policies to them?
- Will you broadcast the SSID of your network?

Defining specific wireless configuration policies for all segments of your network can be complex and time-consuming, which is one reason the U.S. Government Accountability Office (GAO) found that 50%+ of federal agencies surveyed had not taken even this most basic step. With AMP's user interface and IOS configuration templates, it is fast and easy for you to define your basic security policies and ensure that they are applied correctly to all your access points.

While it would be difficult to establish consistent WLAN policies without AMP, it is even more challenging to ensure that all these devices *remain* in compliance with your policies on an ongoing basis. With hundreds or thousands of access points across multiple locations, conducting manual audits of each AP is prohibitively expensive and time-consuming; manual audits simply do not get done. As a result, misconfigurations can go undetected for weeks and even months. This vulnerability, and the difficulty in detecting it, is one reason the Gartner Group has stated that 70% of successful attacks on wireless networks will be the result of a misconfiguration.

"Through 2006, 70% of successful WLAN attacks will occur because of misconfigured access points or client software." (Gartner Group)

AMP virtually eliminates this risk by performing regular, automated audits of your entire Cisco WLAN infrastructure. AMP analyzes the existing configuration file of each AP and compares it to the policies you have defined. If there is any variance, AMP generates an immediate, high-priority alert and provides a link to a report detailing the configuration parameters that are in violation of your policy.

Device Name	Status	Count	Last Audit	Result
wireless-3000-2	Up	0	2 days 4 hrs 36 mins	Mismatched
Cisco350-2	Up	0	82 days 13 hrs 23 mins	Good
cisco1100	Up	0	82 days 11 hrs 41 mins	Mismatched
ap4.corp.airwaves.com	Up	4	5 days 23 hrs 53 mins	Mismatched

AMP allows you to review the configuration errors before taking corrective action, or can be configured to "auto-repair" the configuration as soon as any violation is detected.

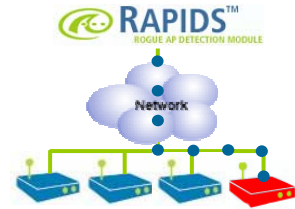
AMP's configuration audit function is superior for several reasons:

- Thorough – AMP routinely audits every Cisco access point on your network at a schedule you define
- Comprehensive – AMP compares the entire configuration file on each AP to the specified policies, highlighting any difference.
- Automated – AMP configuration audits are fully automated, and do not require you to define or initiate a 'job' or manually analyze the results.
- Easy to Comprehend – AMP provides detailed 'mismatch' reports that show you exactly what the configuration *should* be and contrast that with the device's *actual* configuration.

With AMP's configuration audit capability, you can always have confidence that your security policies are being policed and enforced uniformly across your entire network.

Wireline Rogue Access Point Detection: Find the Rogues that Are NOT within Range of your Cisco APs

By now, most security organizations are well aware of the danger posed by unauthorized and unsecured 'rogue' access points connected to the network behind the firewall. The worst-case security scenario is that a malicious intruder installs a rogue AP for the express purpose of invading your secure network resources. By far the most *common* rogue scenario, however, is that well-meaning but naive employees connect access points to your network to get mobile access where no Wi-Fi coverage is yet provided. Very few corporations or large organizations today provide wall-to-wall Wi-Fi coverage in all their facilities, and it is not realistic to assume that 100% coverage will be achieved in the near future. As a result, most organizations have multiple wireless 'dead zones' that are at high risk for employee-installed rogues.



RAPIDS can accurately detect the 100 best-selling access points on Amazon.com using wireline detection techniques alone

The flaw of a rogue detection approach that relies exclusively on your Cisco access points to scan the RF airspace to detect unauthorized devices is immediately obvious. An AP-based wireless detection solution cannot possibly detect rogue access points in precisely the locations where rogues are most likely to be installed: outside the RF coverage area of the authorized APs.

AMP's RAPIDS rogue access point detection module addresses this problem by combining wireless RF detection using Cisco APs (in conjunction with WLSE) with sophisticated scans from the wired side of your network. In this way, RAPIDS can detect and alert you when rogues are found *anywhere* on your network, even if they are far from your existing Cisco APs.

RAPIDS interrogates your routers and switches to obtain the MAC address of every device connected to your network. The software compares this information to its database of 10,000+ MAC ranges assigned to hardware vendors to assess the likelihood that the device is a wireless access point. RAPIDS then launches another set of tests designed to eliminate 'false positive' reports, analyzes the results of all these tests, and assigns each device a score from I-V reflecting the likelihood that it is a rogue AP. A Class V RAPIDS score indicates that the device is definitely an unknown and unmanaged access point, while a Class I score shows no signs of being a rogue AP.

RAPIDS then correlates this data with RF-based information generated by your Cisco APs (if any) and presents all the information on the rogue device to you in a single alert. In this way, RAPIDS helps close the door on one of your most significant wireless security vulnerabilities: the possibility that rogue APs are connected to your network where they cannot be "seen" by other wireless devices. RAPIDS provides the baseline rogue detection functionality that every organization concerned about network security must have in place.

Superior Network Discovery: It's the Access Point You Cannot Find that Should Worry You the Most

While rogue access points are a clear and obvious threat to network security, 'undiscovered' access points may be even more common and harder to detect. If one of your own access points is not discovered by your management solution, you cannot manage the device and cannot possibly ensure that the security policies are configured properly. Even worse, if an intruder uses that device to connect to the network, you may never detect the breach.

AMP provides superior discovery for your Cisco wireless network because it does not rely on CDP alone to identify Cisco (and other) APs on your network. Instead, AMP combines CDP with SNMP and HTTP scans to discover your access points even if they are sitting behind routers or edge switches that do not support CDP. By using all means possible to discover your APs, AMP minimizes the chance that one of your own APs can be used to breach your network.

Detailed User Log Files: Know Who Has Used Your Network

In the event that your wireless LAN is ever subject to an attack, your network security group will need immediate access to forensic data showing who was connected to the network, what bandwidth they used, etc. The speed and accuracy with which you can provide this information will often determine the effectiveness of your organization's response to the attack.

MAC Address	IP	Authentication Time	Duration	Amount
00:0C:29:11:2A:40	10.10.10.10	7/20/2005 7:32 AM	2 mins	0.0
00:0C:29:11:2A:40	10.10.10.10	7/20/2005 8:40 PM	2 hrs 0 mins	0.0
00:0C:29:11:2A:40	10.10.10.10	7/20/2005 11:07 AM	7 hrs 32 mins	35.9
00:0C:29:11:2A:40	10.10.10.10	7/20/2005 11:50 AM	2 hrs 24 mins	4.9
00:0C:29:11:2A:40	10.10.10.10	7/20/2005 7:21 AM	1 hr 43 mins	8.2
00:0C:29:11:2A:40	10.10.10.10	7/20/2005 11:08 PM	1 hr 24 mins	29.7
00:0C:29:11:2A:40	10.10.10.10	7/20/2005 9:17 PM	1 hr 41 mins	0.9
00:0C:29:11:2A:40	10.10.10.10	7/20/2005 7:09 AM	1 hr 6 mins	39.0
00:0C:29:11:2A:40	10.10.10.10	7/20/2005 11:08 AM	1 hr 26 mins	4.3
00:0C:29:11:2A:40	10.10.10.10	7/20/2005 4:41 PM	2 hrs 6 mins	0.8
00:0C:29:11:2A:40	10.10.10.10	7/20/2005 12:03 PM	3 hrs 28 mins	4.2
00:0C:29:11:2A:40	10.10.10.10	7/20/2005 11:54 AM	59 mins	2.4
00:0C:29:11:2A:40	10.10.10.10	7/20/2005 11:42 AM	10 mins	0.0
00:0C:29:11:2A:40	10.10.10.10	7/20/2005 11:05 PM	34 hrs 47 mins	36.2
00:0C:29:11:2A:40	10.10.10.10	7/20/2005 12:46 AM	1 hr 11 mins	1.0
00:0C:29:11:2A:40	10.10.10.10	7/20/2005 12:46 PM	1 hr 36 mins	0.5
00:0C:29:11:2A:40	10.10.10.10	7/20/2005 11:16 AM	1 hr 8 mins	11.8
00:0C:29:11:2A:40	10.10.10.10	7/20/2005 11:14 AM	6 mins	0.0
00:0C:29:11:2A:40	10.10.10.10	7/20/2005 10:46 AM	1 hr 8 mins	1.8

AMP retains detailed historical log files on each device connected to your wireless network for a year or more, and even provides the username associated with that device whenever available. As a result, you can quickly generate detailed session reports on any user, showing when he or she first connected to the network, where he connected, whether/how he authenticated, what bandwidth he used, where he roamed, and more.

Administrative Access: 'Need to Know' Access to Your Network

One of the most basic precepts of network security is that only individuals who "need to know" should have access to network usage data and that only a small group of trained employees should be able to alter the configuration of any network device. Yet, at the same time, individuals ranging from the Help Desk specialists to network engineers and security auditors need to interact with your wireless management system to get the information they need to do their jobs.

AMP provides both security and usability through a multi-layered, password-protected approach to administrative access that gives you the ability to determine exactly what permissions each user should possess:

- Role-based access restrictions – Allows you to provide 'read-only' access to Help Desk and other users while preventing them from making any changes to the network configuration.
- Group-based access restriction – Allows you to restrict users to viewing data from a subset of the network (i.e., a network engineer in the San Francisco campus may see all information from his campus, but not from any other campuses).

All changes recorded in log files by username to ensure accountability, enabling you to determine exactly who authorized any changes to the wireless network.

How Does AirWave Increase My Flexibility?

Integrate Support for Multiple Cisco Product Lines: Aironet plus Airespace

Most organizations, even those with an all-Cisco wireless LAN infrastructure today, need more flexibility than can be provided by a proprietary, single-vendor management solution.

Even if you have and plan to maintain an 'all-Cisco' wireless LAN, your wireless network will inevitably become more complex in the future as the Cisco product lines continue to evolve. In early 2005, Cisco completed the acquisition of Airespace to add WLAN switches to its existing Aironet product line. As enterprises expand their wireless LAN to include WiMax, mesh networking, location-based services, and more over the next several years, Cisco will almost inevitably add new products and product lines.

AirWave's vendor-agnostic common object model for managing multi-vendor hardware also enables it to quickly and efficiently add support for new device types and products from Cisco. This helped AirWave become the first management provider to announce support for both the Cisco Aironet and Airespace product lines, helping customers manage their entire diverse Cisco infrastructure from one integrated console. As Cisco continues to add new products, AirWave's flexible software architecture will continue to deliver a simple common interface from which to manage an increasingly diverse wireless network.

Continued Support for Legacy Devices

The same common object model design that helps AirWave manage the diversity of the current Cisco product line also allows it to maintain superior support for legacy devices that have been 'end-of-lifed' by the hardware vendor.

In designing their management solutions, hardware vendors inherently need to balance the need to support their current products against their customers' needs for ongoing support of existing, 'legacy' hardware. As a result, it is not uncommon for hardware vendors to 'end-of-life' support for hardware products after a period of 2-3 years in order to focus on delivering additional functionality for new hardware. This has the added benefit (from the perspective of the vendor) of encouraging their customer base to upgrade to new hardware on a regular basis.

Yet, for many organizations, wireless LAN equipment is expected to have a much longer lifespan. For a retailer with 3,000 wireless access points in 1,500 physical locations, for example, the cost of replacing hardware in all these locations every two years would be unimaginable. Similarly, in large K-12 school districts where capital budgets are tightly constrained, hardware may be expected to last 5-7 years.

As a third-party management provider, AirWave's sole motivation is to ensure that its customers can manage even the most diverse wireless LANs. AirWave support for the Cisco wireless LAN product line dates back to 2002, including continued support for the Aironet 340 and 350 access points with VxWorks operating system. As a result, AirWave customers have control over their own network and their upgrade cycles rather than having to adhere to a schedule dictated by a vendor.

Manage Your Entire WLAN, not just Your Cisco WLAN

Many large corporations with an 'all-Cisco' infrastructure already have a much more diverse wireless LAN infrastructure than they think. While the IT staff in the corporate NOC may have standardized on Cisco hardware, network engineers in other locations or divisions may already be purchasing hardware from other vendors without their knowledge. More often than not, when AirWave software is installed in an "all-Cisco" network environment at a large corporation, it discovers at least a handful of non-Cisco devices. Assuming that your network is 100% homogeneous can be extremely dangerous: If it is not (for any reason), you may never discover the other devices and cannot ensure that the appropriate policies are enforced. A far more prudent course is to assume that your wireless network is heterogeneous until you can prove to your satisfaction that it is not.

While hardware purchasing and selection decisions in today's global organizations may be somewhat decentralized, network and security policies must be centrally defined and coordinated. With a proprietary, single-vendor management solution, you cannot possibly centrally enforce policies across a multi-vendor environment. As a multi-vendor management solution, AMP gives you the ability to define your policies and ensure they are enforced, no matter what hardware is used.

Prepare for Mergers & Acquisitions

A CIO's job is not just to build a network infrastructure that meets the organization's needs today, but also to anticipate and prepare for its future needs. In today's business climate, a CIO must assume that his corporation will merge with or acquire other organizations in the near future. The CIO's job in a merger is to integrate the different organizations' IT infrastructures and deliver immediate cost savings. As wireless LANs become more prevalent in the corporate world, it is fair to assume that the two organizations will often have large, mission-critical wireless LANs comprised of hardware from different vendors.

In a recent study conducted by Accenture, the success of the IT integration was cited by senior executives as the "the most critical factor in the overall success of a merger – above management and leadership." In the same study, the single greatest impediment to IT integration was "infrastructure incompatibility." (Source: Outlook Journal, June 2005) With the success or failure of future transactions dependent upon his ability to integrate disparate infrastructures and the speed with which he can accomplish this task, no CIO can afford to rely on a proprietary management solution from *any* hardware vendor.

By the time a merger is announced, it is too late to start planning to integrate diverse systems. By providing one solution to manage disparate architectures and products, AirWave provides your organization an insurance policy to ensure that you can manage your wireless network of tomorrow in addition to your WLAN of today.

How Does AirWave Make My Cisco WLAN More Scalable?

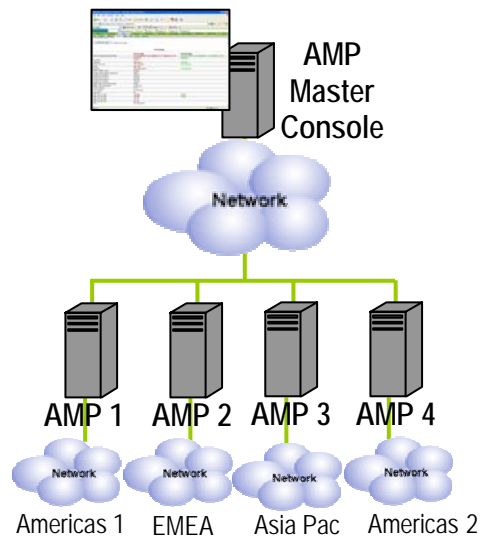
Even most CIOs today do not know for certain how large their wireless network will grow in the next several years. One thing is certain, however: your wireless network (and wireless network usage) will be substantially larger in the future than it is today. Every IT organization must prepare itself for rapid, unpredictable growth and ensure that its management solution will scale for the future. The AirWave Management Platform has been designed to manage even the largest networks, and is used to manage Cisco wireless LANs with 10,000+ wireless APs today.

Scalable Software: No Management "Silos"

AMP's software architecture provides a clear advantage in scalability. A standard server (with two CPUs) running the AirWave software can usually monitor and configure 1,000 or more wireless access points without difficulty. As your wireless network expands, you may add more servers or shift the AMP software to a server with more memory and processing power. Unlike a stand-alone appliance, the constraints of your hardware will never place a hard limit the size of the network you can manage effectively with AMP.

Even if your wireless network has tens of thousands of APs, it is still part of a one single enterprise network. It is unacceptable to have to divide your global Cisco wireless network and manage each segment on a stand-alone basis simply because the management appliance does not scale to the size of your network.

For larger networks that require multiple servers, AirWave provides the AirWave Master Console for integrated management. The Master Console communicates with all the AMP servers and aggregates monitoring data from them, giving you one integrated console from which you can monitor your entire network.



Ultimately, the most important measure of the scalability of your wireless management solution is not the number of APs managed per server or the number of servers that can be added. The true measure of the scalability is whether your solution supports your operational processes cost-effectively.

In terms of true operational scalability, AMP outshines any other solution for managing your Cisco network:

- AMP allows you to divide responsibility for the wireless LAN across your entire IT staff, just as you do with your wired LAN today rather than making a small group of skilled but over-worked network engineers handle all network tasks.
- AMP's simplified and automated processes make it possible to manage thousands of APs with a small IT staff.
- AMP's web-based user interface supports an unlimited number of simultaneous administrative users.
- AMP server-based software can be installed in a centralized NOC, with no local agents

Operational Scalability

or client software required for administrative users.

From its inception, rather than developing 'one-size-fits-all' appliances, AirWave has designed its software to operate the largest wireless networks in the world. Even AirWave's flexible pricing policy allows you to select an appropriate, affordable software solution today while providing a clear upgrade path for the future.

Conclusion

For customers with a Cisco wireless LAN, AirWave's provides an 'insurance policy' that assures them they will be able to manage a more complex, diverse wireless network in the future can be critically important. Even more important, however, is the fact that the AirWave Management Platform will make their Cisco wireless LANs

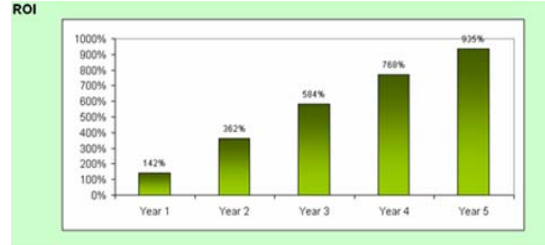
more secure and to reduce their operating costs *today*. In fact, AirWave typically finds that Cisco customers experience a positive ROI in the AirWave software within 6-12 months, even if they have already purchased the Cisco WLSE appliance.

By reducing network operating costs, AirWave also helps improve network performance and user satisfaction. Instead of performing mundane and routine tasks, network engineers' time is freed to work on improving overall network design and evolving the network to handle increasing usage. Users experience better performance, have fewer difficulties getting connected, and problems are resolved on the first call to the Help Desk.

With AMP, your Cisco wireless LAN will fulfill the expectations you had when you purchased and installed your first Wi-Fi network. You'll be able to deliver secure mobility to your users without overwhelming your IT staff and infrastructure. In the end, AMP offers the best management value for your Cisco wireless LAN.

If you're interested in learning more about the AirWave Management Platform, or in seeing a live, one-on-one web-based demonstration of the AMP software with an AirWave network engineer, please contact:

AirWave Wireless Inc.
info@airwave.com
866-802-1121 (in the U.S.)
+1.650.286.6100 (international)



A Typical ROI Result for AMP