

# Aruba-Airwave Solution Sheet

Partner Solution Brief

## TABLE OF CONTENTS

Introduction .....	2
Aruba-AirWave Integrated Solution.....	3
Reduced Cost & Complexity .....	3
Enhanced Security .....	3
Complete Manageability and Flexibility.....	4
Typical Deployment: Small to Medium Wireless Network .....	5
<i>Network Design Parameters</i> .....	6
Typical Deployment: Large, Distributed Wireless Network .....	6
<i>Network Design Parameters</i> .....	7
Summary .....	7

## Introduction

The advent of centralized WLAN architecture has significantly increased the adoption of WLAN technology in the enterprise. However many organizations have already made large investments in traditional wireless LAN deployments using “fat” (or “stand-alone”) access points from various hardware vendors including Cisco, Symbol, and others. In fact, more than 5 million stand-alone access points have already been purchased by enterprises today, representing billions of dollars of pre-existing Wi-Fi investments<sup>1</sup>.

Many of these organizations now wish to transition to a centralized architecture for enhanced security, fast roaming (for voice and other mobile applications), and other new applications like guest access. Until now, these organizations have had limited, unappealing options:

- “Do Nothing” - Continue to implement fat access points that do not fully meet the organization’s new requirements
- “Rip & Replace” - Replace the entire existing Wi-Fi infrastructure with new hardware, at great expense
- “Management Silos” - Leave the existing infrastructure in place and migrate to a centralized infrastructure for new installations, forcing the IT staff to use separate management systems to control the new and legacy infrastructure.
- “Brain Transplant” - Convert some legacy access points to “thin” (LWAPP) APs via a time-consuming upgrade process, while replacing older access points that cannot be upgraded.

Option	Meets New WLAN Security & Mobility Requirements?	Complexity	Cost
Do Nothing	No	High	High
“Rip & Replace”	Yes	Low	Very High
“Management Silos”	Yes	High	Very High
“Brain Transplant”	Partial	Very High	Very High

**Table 1**

The Aruba-AirWave partnership provides these customers with a better, evolutionary alternative that is more cost-effective and less disruptive. Aruba’s Mobile Edge products deliver all the benefits of a centralized architecture while the AirWave Wireless Management Suite provides comprehensive management of the entire wireless LAN infrastructure, including legacy “fat” access points from other vendors.

---

<sup>1</sup> Dell’Oro Group, January 2006.

## Aruba-AirWave Integrated Solution

The Aruba-AirWave partnership delivers key benefits *to a broad set of customers* with existing wireless LAN installations *across* multiple vertical markets, including *education, healthcare, retail, and manufacturing.*

### *Reduced Cost & Complexity*

- Extends the life of existing Wi-Fi hardware by years, reducing capital expenditures and installation costs. The AirWave Management Platform (AMP) software provides full support for stand-alone access points from multiple vendors, including Cisco, Symbol, Proxim, Enterasys, Avaya, HP ProCurve, and more. This means that customers can fully control both new and legacy hardware from the same console. On average, AirWave customers report that the AMP platform allows them to extend the life of legacy hardware by 15 months, and often by two years or more.<sup>2</sup>
- Eliminates risky and time-consuming software upgrades to existing hardware. By using Aruba controllers with a flexible management solution that supports both stand-alone and thin APs, customers do not have to 'upgrade' their legacy APs to LWAPP to get the advantages of a centralized architecture.
- One management console for the entire network. With the AirWave Management platform, organizations with a diverse wireless infrastructure do not need separate consoles for 'fat' and 'centralized' infrastructure, or for products from different vendors. This dramatically reduces training costs and gives the IT staff one console for monitoring the entire network, reducing support costs and simplifying network planning.

### *Enhanced Security*

- *User-based policy enforcement* via Aruba controllers, enabling the organization to control exactly who can access the network and what privileges they receive. All the wireless traffic is scanned by the Aruba controller to provide per-user policy-based access control. This enables applications such as voice and guest access to be enabled on the legacy and Aruba wireless infrastructure. Wireless users benefit from a uniform experience across legacy and Aruba infrastructure as well as the seamless mobility across the wireless network. (See **implementation details for Small-Medium and Large wireless LANs** below).
- *Centralized encryption architecture* to ensure that enterprise data is protected across both the wired and wireless networks. With Aruba's Mobile Edge architecture, all encryption (including layer 2) occurs at the controller, thereby increasing the security of data on the wired network (as traffic remains natively encrypted between the access point and the controller). This advantage can be retained across legacy access points by the use of the xSec protocol. This protocol is derived from the 802.11i standard and provides the capability to form to a secure tunnel from the wireless client to the controller over Aruba and legacy access points.
- *Automated configuration audit and auto-repair to ensure that security policies are always uniformly enforced across both the legacy and new Wi-Fi infrastructure.* Gartner Group estimates that 90% of wireless security incidents will result from improperly configured infrastructure and devices.<sup>3</sup> The AirWave Management Platform mitigates this risk by continually comparing the actual configuration of legacy and Aruba Wi-Fi devices to the organization's centrally defined policies. If violations are

---

<sup>2</sup> AirWave Customer Survey, June 2006.

<sup>3</sup> John Pescatore, Gartner Group, 2006.

detected, AMP alerts the IT staff and can automatically 'repair' the device configuration to match the organization's policies.

- *Wireless IDS and rogue AP detection to ensure that no unauthorized users connect to the wireless network.* AirWave's RAPIDS software module uses wireless data from legacy and Aruba wireless access points to detect and triangulate the location of any unauthorized rogue access points within range. RAPIDS also scans the organization's wired network infrastructure to find any rogue devices that are not within range of an authorized, managed AP. For optimal security, organizations can install a small number of Aruba APs acting as "Air Monitors" in the vicinity of existing legacy APs for true wireless IDS. Since Air Monitors typically need a much sparser deployment to provide the wireless IDS functionality, most locations with legacy wireless hardware can be secured without significant increase in deployment or operational cost (compared with deploying and maintaining a separate Wireless IDS-only solution)
- *Role-based administrative access to ensure that only IT employees with a "need-to-know" can view network information or change configuration policies.* AMP uses a multi-layered role-based administrative access model to ensure that users receive only the level of access they require to do their jobs. For example, Help Desk users may be given rights to view monitoring data for end-user troubleshooting but not be permitted to view or change configuration policies. A network engineer with responsibility for the wireless LAN in North America may receive configuration privileges for North American infrastructure, but no access to devices in EMEA.

## Complete Manageability and Flexibility

- Real-time views for every user and device anywhere on the wireless LAN. AMP provides detailed real-time monitoring of each device (legacy or new) on the wireless network, giving the Help Desk and Network Engineers access to critical monitoring data for faster problem resolution. With a

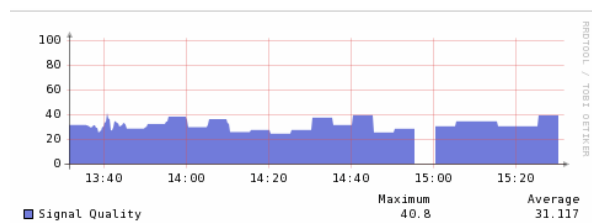


Figure 1. AirWave User Signal Quality View

few mouse-clicks, IT can locate any user on an accurate location map, assess his or her signal quality and bandwidth utilization, see whether there are any RF errors, and determine whether other users connected to that AP are experiencing similar problems. With instant access to this information, AirWave users achieve up to 75% reduction in wireless problem resolution time and up to 50% reduction in overall wireless support calls.<sup>4</sup>

- Automated, centralized configuration management and firmware distribution across new and legacy Wi-Fi infrastructure to reduce time spent on routine tasks. **With AMP, organizations define configuration policies and minimum firmware standards for new and legacy environments centrally. AMP applies the policies across the entire infrastructure, dramatically reducing support costs and eliminating opportunities for human error.**
- Usability for the entire IT staff. AMP's web-based user interface is easy to use for skilled network engineers, Help Desk personnel, security auditors, and other IT staff members. By giving the Help Desk the tools it requires, AMP dramatically reduces the support workload for over-worked (and highly compensated) engineers, freeing them to focus on other IT priorities.

<sup>4</sup> AirWave Customer Survey, June 2006.

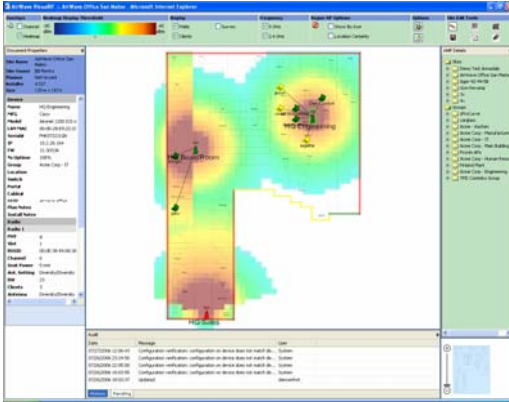


Figure 2. AirWave RF Heatmap & User Location

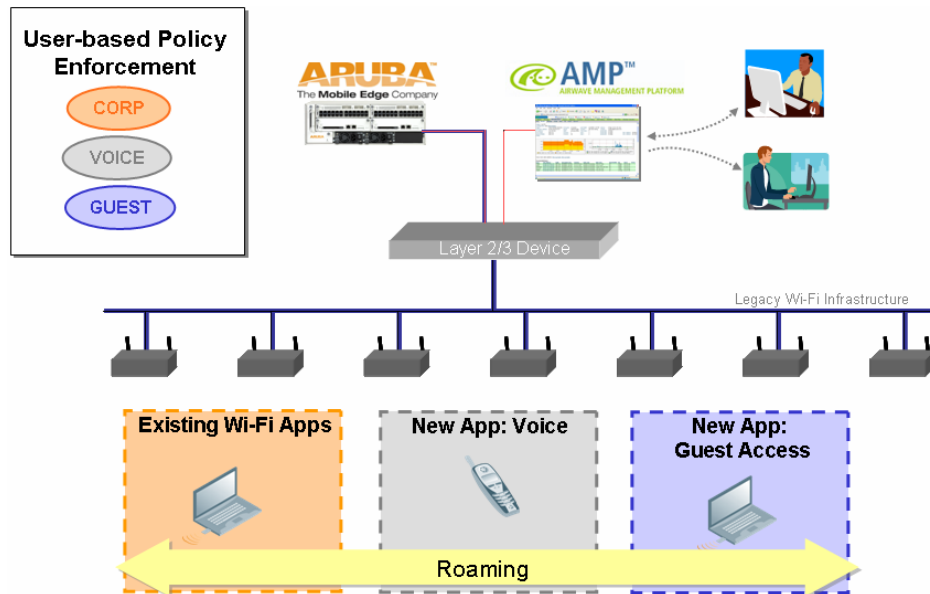
- *Avoid vendor lock-in.* With multi-vendor management capabilities, organizations with the Aruba-AirWave solution avoid vendor lock-in and can always select the hardware platform that best meets their needs, now and in the future. And, with more than 10,500 mergers and acquisitions in the U.S. alone in 2005<sup>5</sup>, these organizations are always prepared to integrate an even more diverse wireless infrastructure in the future, if required.
- *Scalability to handle the largest and most distributed wireless networks in the world.* With wireless networks growing in size and with usage expanding even more rapidly, organizations need to be prepared to manage much larger networks in the future. Aruba has a full line of wireless products to handle any size network. With AirWave's Master Console, even organizations with 20,000 or more wireless access points can monitor the entire network from a single integrated console.

### *Typical Deployment: Small to Medium Wireless Network*

Aruba's Mobile Edge architecture provides sophisticated identity-based security features to enable applications such as secure guest access and role-based security for wireless networks. In a small to medium size wireless LAN, with the deployment model shown below, these advanced security features can be extended to legacy access points as well as Aruba infrastructure.

---

<sup>5</sup> Factset MergerStat



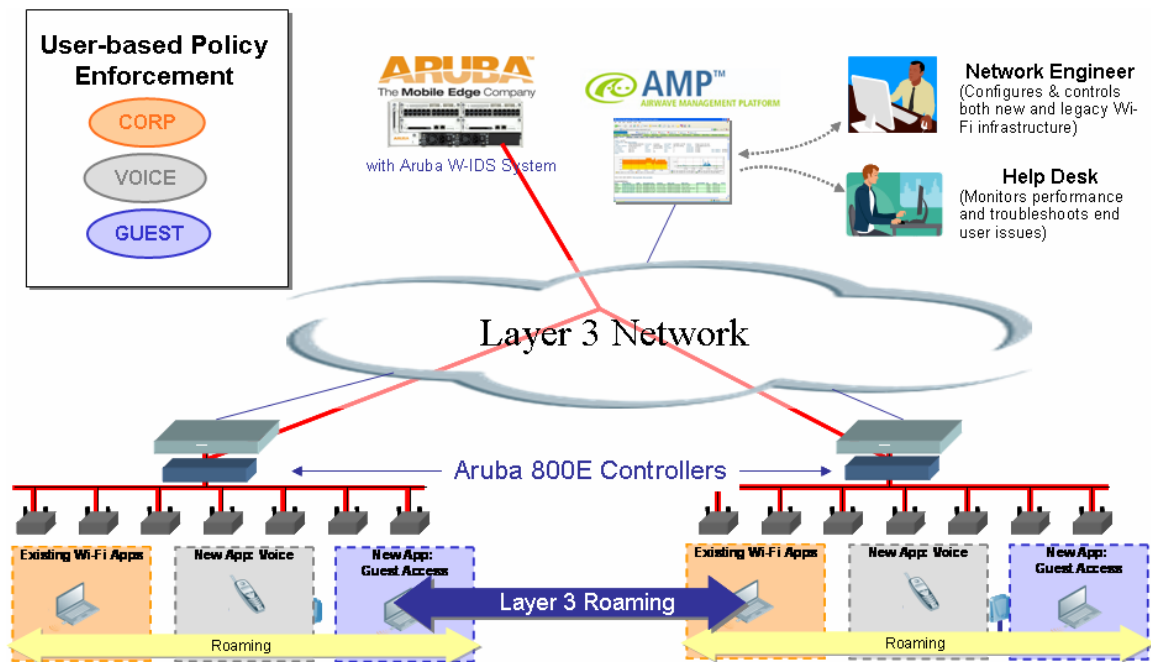
**Figure 3**

## Network Design Parameters

- Wireless user traffic is directed from the legacy AP through the Aruba mobility controller. The organization configures one of the VLAN interfaces of the mobility controller in the same VLAN as the wireless users from the legacy APs. The mobility controller's VLAN interface serves as the default gateway for users in this subnet. This enables new applications such as voice and guest access on both the legacy and Aruba wireless infrastructure.
- AMP configures both legacy and Aruba APs with the same SSID and 802.11 security type. This enables clients to roam across the different types of APs seamlessly. In addition, the proxy-mobile IP implementation on the Aruba controller provides inter-subnet roaming for the mobile users. This is extremely important for most mobile applications, especially voice.
- All encryption is centralized at the Aruba controller, protecting data on the wired network as well as the wireless network.

### *Typical Deployment: Large, Distributed Wireless Network*

In large-scale distributed wireless networks, it may not be possible or practical to make network modifications to redirect all legacy APs to the Aruba controller (as in a small to medium-sized network). To deliver the security advantages of the centralized Aruba architecture, Aruba offers these larger organizations a solution using the 800-E and 2400-E access controllers in addition to the mobility controllers. This is an easy-to-deploy overlay solution that can redirect the legacy APs to the centralized Aruba controllers without having to extend VLANs across large portions of the network.



**Figure 4**

## Network Design Parameters

- 800-E and 2400-E act as access controllers that tunnel all traffic from legacy APs to the centralized Aruba mobility controller in a GRE tunnel. This provides an easy-to-deploy overlay solution for connecting legacy access points to the Aruba controllers without significantly re-engineering the entire network.
- The central Aruba mobility controllers provides the user based policy enforcement for all users across the legacy and Aruba APs
- The solution provides seamless layer 2 and 3 mobility across both legacy and Aruba APs
- Aruba Air Monitors provide Wireless IDS and Location capabilities, even in geographical locations where the legacy APs provide wireless access.

## Summary

As discussed earlier in the document, customers who have made a significant investment in legacy fat access points from various vendors have been stranded with the industry-wide shift to centralized WLAN architectures. The options offered to the customers to migrate to the centralized WLAN architecture have been extremely cost-prohibitive and/or disruptive. The new Aruba-AirWave partnership provides a 'Nondisruptive Overlay' solution that delivers all the advantages of the centralized architecture without requiring a costly upgrade to the network infrastructure.

Option	Meets New WLAN Security & Mobility Requirements?	Complexity	Cost
Do Nothing	No	High	High
"Rip & Replace "	Yes	Low	Very High
"Management Silos"	Yes	High	Very High
"Brain Transplant "	Partial	Very High	Very High
Nondisruptive Overlay	Yes	Low	Low/Medium

**Table 2**

The Aruba-AirWave joint solution provides enterprises that have a distributed WLAN architecture consisting of "thick" access points a migration path to the Mobile Edge, a centralized WLAN architecture. The integration combines the best-in-class security and mobility features from Aruba with the AirWave's management solution to provide a single console for legacy access points and centralized WLAN solutions.



- User-based policy enforcement
- Centralized encryption architecture for added security
- Seamless mobility across legacy and Aruba access points to support voice and other new applications
- Guest access
- Wireless IDS via Aruba "Air Monitors"
- Dynamic RF management for Aruba APs

- Real-time user & device monitoring
- RF Visualization and location information for legacy and Aruba APs
- Single point of control for centralized management of both Aruba and legacy Wi-Fi hardware
- Automated configuration audit
- Role-based administrative access
- Rogue AP detection via both wireless (AP) and wired network scans
- Easy-to-use interface for Help Desk and network engineers