

Enterprise



**Integrating Wired IDS with Wi-Fi
Using Open-Source IDS to Complement a
Wireless IDS/IPS Deployment**

Josh Wright | Senior Security Researcher

Introduction

To address security concerns in wireless LAN deployments, many organizations have deployed Wireless Intrusion Detection Systems (WIDS) to monitor wireless activity for signs of attack. Deployed as an integrated monitoring system with the wireless transport network or as an overlay monitoring system separate from the wireless transport network, these systems are effective at analyzing wireless activity and identifying wireless attackers. Focusing their analysis on the data-link and physical layers of the OSI model (Layers 2 and 1), these tools allow organizations to successfully identify and defend against rogue APs, wireless protocol attacks and denial of service attacks.

While WIDS systems are effective at identifying wireless attacks, they are limited in their ability to identify upper-layer attacks that are traditionally identified with wired IDS tools. This weakness can severely expose wireless network deployments, giving the attacker an opportunity to exploit the wireless network with little risk of being identified by a wired or wireless IDS system.

Fortunately, advanced wireless LAN architectures can employ tactics to overcome the limitations that prevent traditional WIDS systems from extending their analysis to the upper layers of the OSI model by integrating with wired IDS tools including Snort. When used with a mobility controller (MC) for the deployment of access points, customers can take advantage of Snort's powerful rules language to identify attacks on the wireless network and dynamically change access permissions for misbehaving clients while offering unprecedented monitoring capabilities.

This whitepaper will examine the weaknesses and challenges in using traditional WIDS systems to attempt to monitor the upper layers of the OSI model, and will identify techniques used by attackers to exploit weaknesses in WIDS systems. We will also examine how an Aruba Networks Mobile Edge architecture can extend to include upper-layer OSI monitoring using Snort while leveraging role-based access policy enforcement.

Limitations in WIDS Monitoring

Wireless Intrusion Detection Systems are designed primarily to identify attacks affecting the physical and MAC layers (Layers 1 and 2) of the OSI model. For example, analyzing statistical information at the physical layer can indicate RF jamming attacks designed to cause a denial of service attack against a target network. Assessing IEEE 802.11 frame content at the MAC layer can indicate active WEP attacks designed to break weak encryption mechanisms. However, adversaries are not limited to targeting Layer

1 and Layer 2 vulnerabilities when attacking the wireless network, and can extend their attacks to upper layers of the OSI model. This modification in the attack technique exposes several weaknesses in pure wireless IDS systems.

Monitoring Weaknesses

Traditional WIDS deployments make use of access points or air monitors to collect information about traffic on the wireless network. This traffic information can then be used to identify attacks. These embedded platform systems are often designed with lightweight processors to limit the cost for customer deployment. As a result, only limited processing resources are available to perform detailed packet inspection. In a traditional IDS system, servers with significant resources often are deployed to monitor wired links exceeding 100 Mbps. It is not realistic to expect an embedded device, such as an access point or air monitor, to be capable of performing the same analysis for a wireless LAN, on which traffic can achieve rates of 54 Mbps (IEEE 802.11a, IEEE 802.11g).

As an alternative, some organizations deploy traditional wired IDS systems to monitor all traffic as it leaves an access point. By deploying the IDS at a traffic aggregation point, organizations can monitor the traffic for several access points as shown in Figure 1.

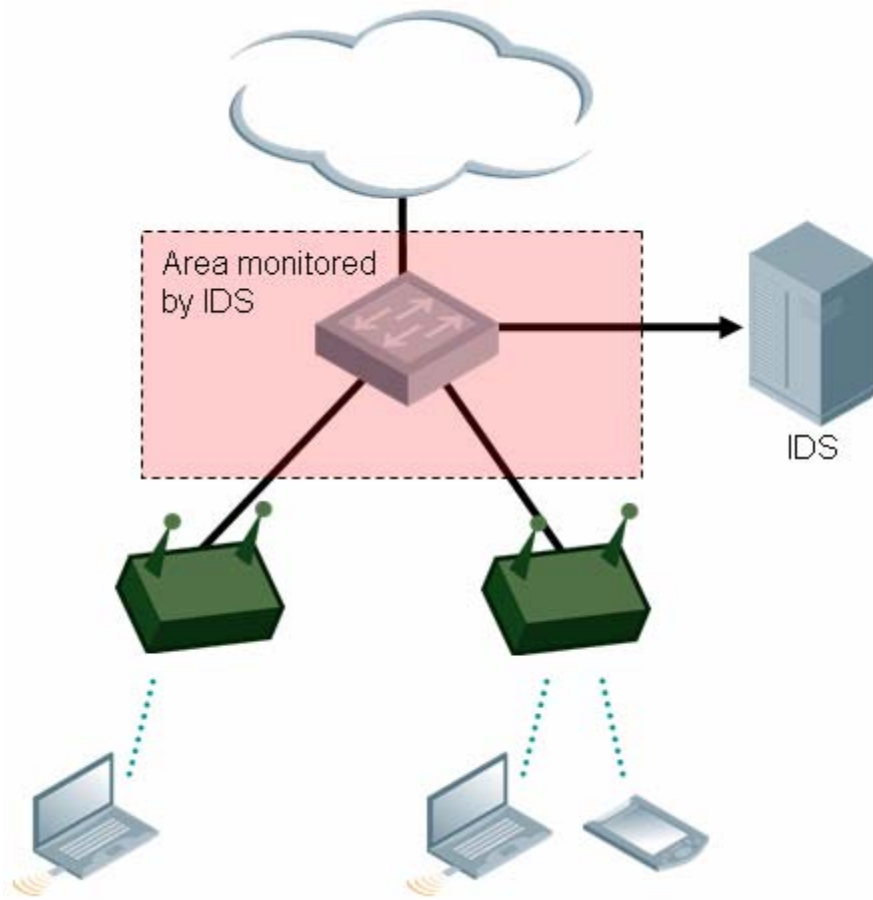


Figure 1. Augmenting WLAN with Wired IDS Monitoring

In this deployment, the IDS system can monitor all activity leaving and entering the wireless network and identify potential misbehavior, including intrusions, worms and other malicious activity. While this deployment is effective at monitoring the traffic entering and leaving the wireless network, it is incapable of monitoring activity on the WLAN itself, and exposes the network to attacks that do not traverse the wired network, as shown in Figure 2.

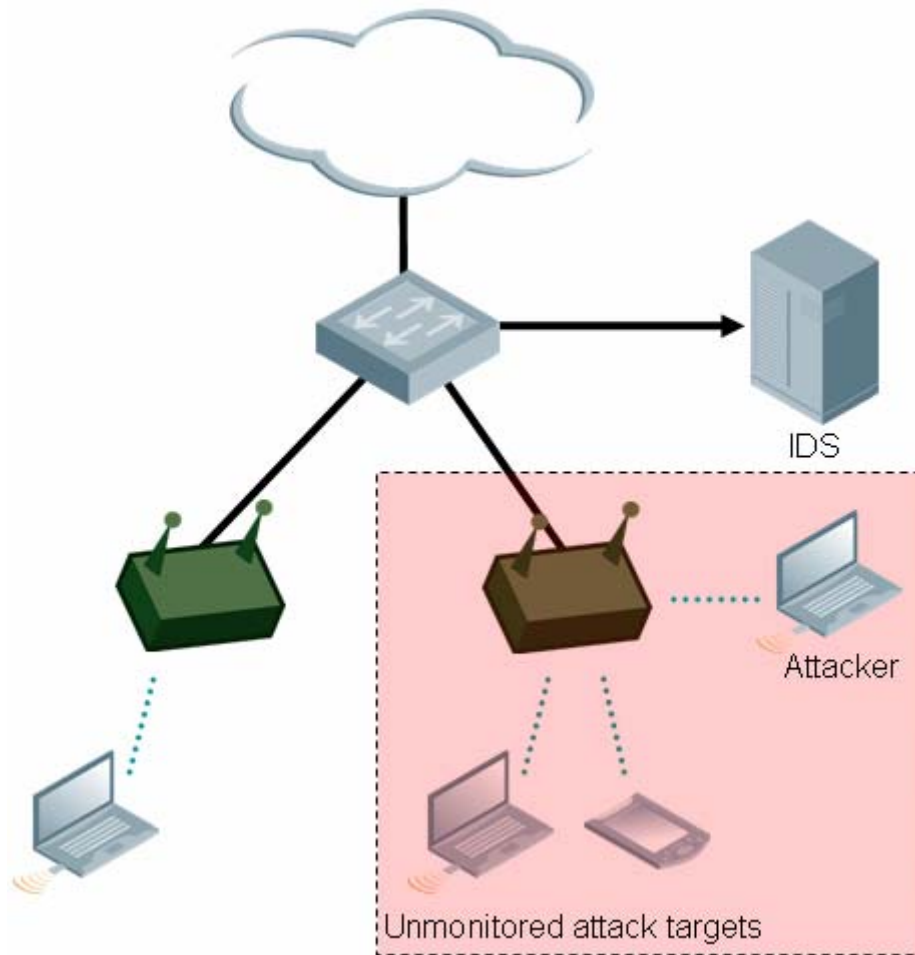


Figure 2. Exposure of unmonitored attack targets on a WLAN.

When the wired IDS is deployed at a network aggregation point, it is unable to assess any traffic that does not traverse the aggregation point, including all local WLAN traffic. When an attacker can associate himself with the WLAN, as in the case of an open network or a closed network with the proper authentication credentials (an insider attack), he is able to target any local WLAN devices without the risk of being detected by the wired IDS system.

Traffic Analysis Weaknesses

Another significant weakness in traditional WIDS systems is the inability to monitor the contents of any network traffic that is protected with dynamic encryption keys. In modern encryption mechanisms used on

wireless networks, the access point and the client derive unique key information for each session, which protects subsequent data in that session from traffic sniffing attacks. In order to sufficiently protect the confidentiality of the network traffic, only the client station and the access point are privy to the dynamic keys used for encryption and decryption.

An air monitor deployed as an overlay to the wireless network is able to inspect the contents of the unencrypted MAC layer to identify some attacks on the wireless network, but is unable to decrypt the payload of data frames without knowledge of dynamic key information. This limitation prevents an overlay WIDS deployment from examining upper-layer protocol traffic including IP and TCP packets.

WIPS Limitations

Many WIDS systems also claim to offer wireless intrusion prevention (WIPS) mechanisms designed not only to identify attacks on the wireless network, but also to stop an attack from being successful. This is often achieved by utilizing well-known denial-of-service (DoS) attacks applicable to IEEE 802.11 networks against an identified attacker. Typically launched from the air monitor device, the DoS attack forces the attacker to repeatedly disconnect from the network after receiving de-authentication and disassociation frames on behalf of the local access point.

While this technique is currently useful for a limited number of WIPS mechanisms, it is far from a comprehensive intrusion prevention mechanism. In order to stop an attacker from communicating on the wireless network, a local air-monitor device must send spoofed de-authenticate and/or disassociate frames to the attacker while appearing to be from the legitimate access point. These frames must be transmitted rapidly, since the target station will attempt to reconnect to the network rapidly, which contribute to overall congestion and overhead on the wireless network.

Further, the air-monitor loses its ability to rapidly scan other channels for attacks while currently engaged in a DoS attack with an attacker. This could be leveraged as a "bait-and-switch" WIDS evasion technique by the attacker who could impose a rogue AP on the network to demand the focused attention of an air-monitor device. Meanwhile, another system or a separate wireless card could be used to attack another access point on a different channel.

Finally, emerging standards will likely hinder the productivity of common WIDS practices. When ratified, the IEEE 802.11w amendment by the IEEE will provide support for protecting the integrity and confidentiality of 802.11 management traffic. The current draft of the IEEE 802.11w amendment will also provide integrity protection and replay protection for both de-authenticate and disassociate frames in an effort to mitigate DoS attacks on wireless networks. As access points and wireless drivers are updated to include the protective mechanisms offered by the IEEE 802.11w amendment, the de-authenticate and

disassociate approach for WIPS will no longer be effective since AP's and client systems will reject the air-monitor's traffic.

Taking a New Approach to WIDS

The Aruba Networks Mobile Edge architecture, implemented with a Mobility Controller, thin access points and air monitor devices, provides the administrator with unique features that effectively mitigate many of the weaknesses that afflict traditional overlay WIDS systems or other integrated transport and monitoring systems.

Centralized Monitoring

Unlike other thin-AP wireless network deployments, the Aruba architecture uses a centralized encryption and decryption mechanism whereby all traffic is forwarded from the AP to the Aruba MC for processing. This feature allows administrators to take advantage of centralized, high-speed encryption and decryption processors, while aggregating wireless traffic from all access points at the mobility controller. Where a traditional thin-AP architecture offloads wireless traffic at the access point, the Aruba solution aggregates all traffic and therefore is able to monitor wireless activity for all stations at the mobility controller. This approach allows an administrator to deploy a single wired IDS system to monitor all traffic originating from the wireless network, even traffic that is sent only to other wireless stations.

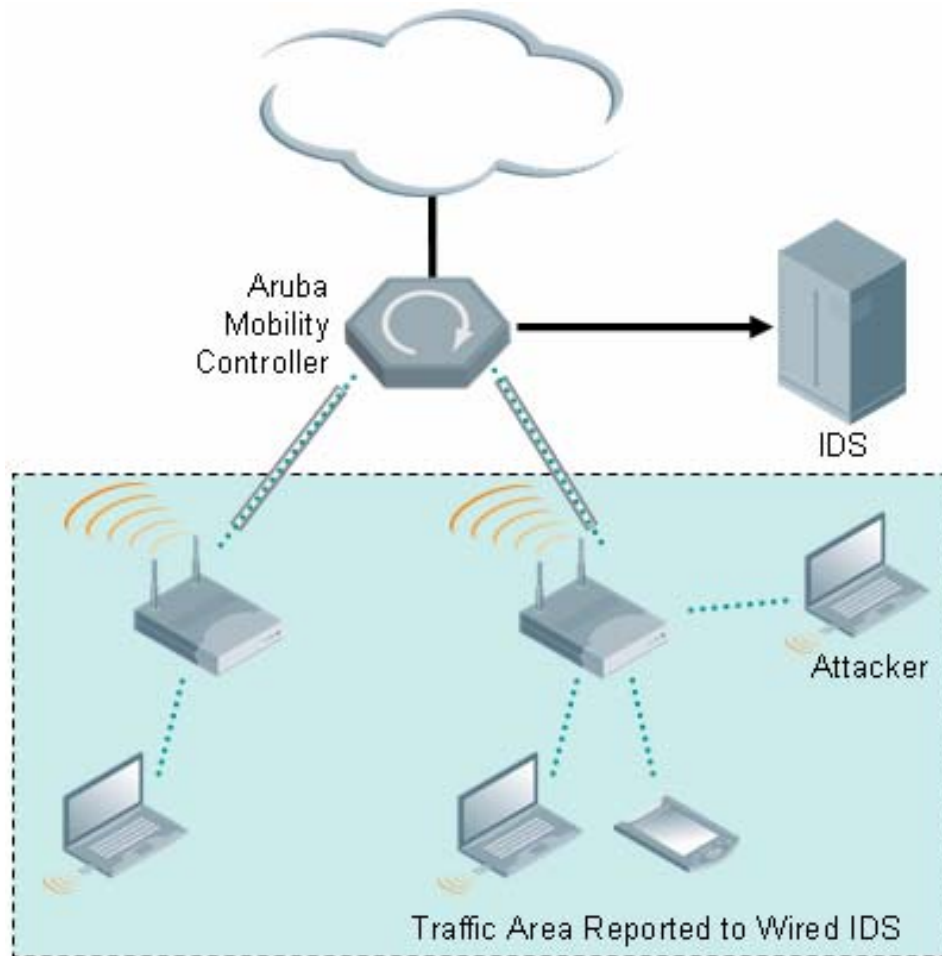


Figure 3. Comprehensive wireless traffic monitoring for the WLAN.

Extended Traffic Analysis

Where an overlay WIDS system is only capable of examining traffic at Layers 1 and 2 of the OSI model, the Aruba centralized encryption architecture accommodates a more capable and flexible traffic analysis model. Since all wireless traffic is encrypted and decrypted with a dedicated cryptographic accelerator on the Aruba MC, the MC has knowledge of all dynamic encryption and decryption keys and can decrypt traffic as needed for upper-layer analysis. In this model, combined with the aggregated monitoring features with centralized encryption, the Aruba MC can easily integrate with upper-layer IDS systems for intrusion analysis at all layers of the OSI model, not just Layer 1 and Layer 2.

Role Based Policy Enforcement

While it is sometimes necessary to invoke wireless DoS attacks for wireless intrusion prevention, an integrated transport and monitoring system such as the Aruba MC can provide a much more flexible and effective mechanism for stopping attacks on the wireless network. Further, these features can be extended to accommodate policy-enforcement on the wireless network as well.

When the Aruba MC is deployed as the transport and monitoring system, administrators can take advantage of flexible and powerful role-based access control mechanisms to grant or restrict access to network resources based on the requirements of the network. The Aruba MC controller integrates an ICSA-based stateful firewall, allowing policy-based roles to be established for users and devices. Roles can be granted based on username, SSID, wireless encryption mechanism, user physical location or other externally-influenced factors such as group membership in an LDAP directory. From the perspective of the monitoring system, if a network access violation is detected (for example, the use of a forbidden protocol such as FTP on a network designated only for voice traffic), the privileges of the user can be revoked (blacklisted), or the user can be assigned a different role.

Further, the benefits of role-based access controls are not limited to use with Aruba products. Using an openly documented XML-based API, third-party systems can easily integrate with the ArubaOS. This enables the third-party systems to dynamically change the roles and privileges of authenticated wireless users, giving them the capability to grant, revoke or restrict access to any internal or external networks. This allows administrators to easily expand monitoring systems by adding network access controls that can protect end-users and internal networks from attacks, and can enforce policy requirements on the network. For example, a network-based anti-virus scanning system can easily be extended to communicate with the Aruba MC and dynamically change the access privileges of users who are suspected of being infected. Such users could have access to external or sensitive systems revoked but could still be granted access to patch-management and anti-virus update services.

Where 802.11-based DoS attacks are of limited effectiveness and may require the network to make trade-offs in performance, role-based access control offers increased reliability and a higher level of flexibility in terms of how network security policy violations are treated.

Deployment Case Studies

In order to better illustrate the strengths of the Aruba Mobile Edge deployment architecture for a secure wireless network, we can examine deployment case studies that take advantage of these features for powerful security solutions.

Extending WIDS with Wired IDS

While many organizations have deployed wired IDS systems, few have extended this monitoring to their wireless networks. Unlike wireless IDS systems, a wired IDS system focuses on the analysis of OSI model Layers 3 and higher, and is effective at identifying attacks that target software vulnerabilities and other network policy violations.

The following three requirements are essential for successfully integrating the wired IDS with the wireless network:

The solution must mirror a copy of unencrypted wireless traffic to the wired IDS for analysis;

The solution must facilitate monitoring of all wireless networks with a single wired IDS sensor, up to the bandwidth and capacity constraints of the networks that are being monitored;

The solution must provide protective measures to enforce policy requirements for network usage by modifying the offending user's wireless privileges, or by stopping all network access.

The open-source wired IDS tool Snort was selected for integration because it is the world's most widely deployed IDS system. Another consideration was the wide availability of the source code required to apply the changes that were necessary to integrate Snort with the Aruba mobility controller.

The Snort IDS is well-known for its powerful rules language, which is designed to decode and inspect traffic with speed and flexibility. Whenever the Snort sensor observes a matching condition between a rule and observed traffic, it takes an action based upon the configuration specified by the administrator. This action can be to log the activity to a database, to generate an email message to an SMS paging system, to generate a syslog event, or any combination of several events. The ability to take an arbitrary action based on a matching alert by the Snort sensor is a function of Snort's output plug-in facility.

Figure 4 illustrates the network architecture that was established for deploying the integrated Aruba mobility controller and Snort sensor.

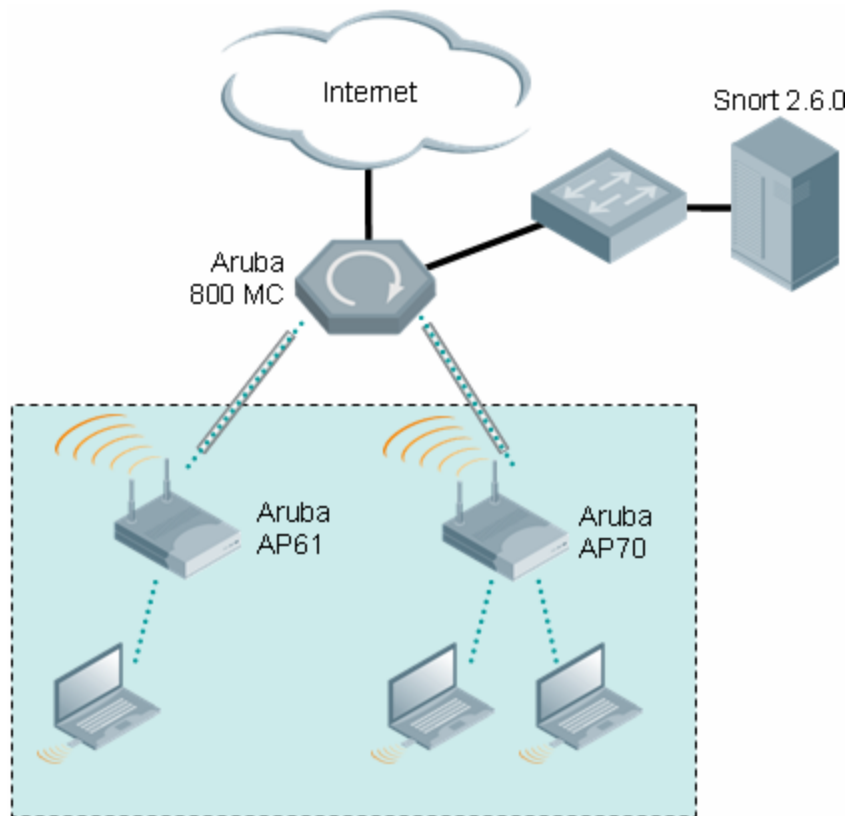


Figure 4. Simplified network deployment example for Aruba mobility controller and Snort integration.

Traffic Mirroring

In order to meet requirements 1 and 2, it was not feasible to physically attach the Snort sensor to the Aruba MC. While this is a supported feature in ArubaOS, it was determined that this would be an atypical deployment scenario. Instead, it is a desirable property of the integrated system to leverage an existing Snort sensor for monitoring wireless network traffic.

Therefore, while the Aruba mobility controller observes all wireless traffic from the three users in Figure 4, the challenge was to mirror a copy of the unencrypted wireless frames to the Snort sensor over the network. The solution was to leverage the ArubaOS session mirror feature to copy all traffic that is received by the Aruba MC into a GRE tunnel directed at the Snort sensor. This allows one or more Aruba MC's to deliver a stream of traffic to the Snort sensor for analysis regardless of the physical placement on the network.

Leveraging Network Access Controls

In order to meet requirement 3, the Aruba MC must be able to influence the network access privileges and rights based on analysis of the Snort sensor using designated rules. The desirable outcome here is that for any condition met by analyzing traffic with the Snort rules language, the Snort sensor should direct the Aruba MC to take a specified action against the offending source, such as restricting or revoking wireless network access privileges.

In order to satisfy this requirement, a Snort output plug-in--designated "alert_aruba_action"--was written and contributed to the Snort project under the terms of the GNU Public License (GPL). With it, Snort users can leverage any Snort rules and, when triggered by a network event, can modify or revoke privileges for the offending wireless user by changing the user's role on the Aruba MC. The Aruba Action output plug-in for Snort is included in the official Snort distribution, version 2.6.1 and later.

Conclusion

As the security for wireless networks has become more resilient, attackers have modified their techniques to exploit other weaknesses, including targeting vulnerable stations at the upper layers of the OSI model. These next-generation attacks are difficult to identify with disjointed overlay monitoring systems that are not an integral part of the wireless transport mechanism. Even traditional WLAN deployments are unable to utilize wired IDS systems to monitor these networks in a comprehensive and scaleable fashion.

As we have shown, the centralized encryption benefits of the Aruba Mobile Edge network allows an organization to integrate a traditional IDS system, such as Snort, with the wireless network for comprehensive and unparalleled monitoring capabilities.

About Aruba Networks, Inc.

Aruba securely delivers the enterprise network to users, wherever they work or roam, with user-centric networks that significantly expand the reach of traditional port-centric networks. User-centric networks integrate adaptive WLANs, identity-based security, and application continuity services into a cohesive, high-performance system that can be easily deployed as an overlay on top of existing network infrastructure. Adaptive WLANs deliver high-performance, follow-me connectivity so users are always within reach of mission-critical information. Identity-based security associates access policies with users, not ports, to enable follow-me security that is enforced regardless of access method or location. Application continuity services enable follow-me applications that can be seamlessly accessed across WLAN and cellular networks. The cost, convenience, and security benefits of user-centric networks are fundamentally changing how and where we work. Listed on the NASDAQ and Russell 2000® Index, Aruba is based in Sunnyvale, California, and has operations throughout the Americas, Europe, Middle East, and Asia Pacific regions. To learn more, visit Aruba at <http://www.arubanetworks.com>.

© 2007 Aruba Networks, Inc. All rights reserved. Specifications are subject to change without notice.

Aruba Networks, BlueScanner and RFprotect are trademarks of Aruba Networks, Inc. All other trademarks or registered trademarks are the property of their respective holders.

WP_IDS_US_071217



1322 Crossman Ave. Sunnyvale, CA 94089-1113
Tel. +1.408.227.4500 | Fax. +1.408.227.4550 | info@arubanetworks.com
<http://www.arubanetworks.com>