

# Managing Secure Wireless LANs:

## The Inextricable Link Between Wireless Network Security and Network Management

---

### Contents

<b>Wi-Fi Security: The Basic Requirements .....</b>	<b>2</b>
1) Data Encryption.....	2
2) Authentication & Access Control.....	2
3) Intrusion Detection .....	2
4) Wireless Network Management .....	2
<b>Wireless Data Encryption .....</b>	<b>2</b>
<b>Authentication and Access Control.....</b>	<b>3</b>
<b>Intrusion Detection.....</b>	<b>3</b>
Wired Network Scans.....	4
Wireless Network Scans .....	4
<b>Wireless Network Management.....</b>	<b>5</b>
Network Discovery .....	5
Automated Configuration.....	5
Audit Management .....	6
Firmware Management .....	6
Network Monitoring & Alerting.....	6
<b>Conclusion.....</b>	<b>7</b>

---

Wireless network security is increasingly becoming an executive-level issue in enterprises and other large organizations due to concerns about Sarbanes Oxley, HIPAA, Visa's CISP program, and other regulations. IT security experts have focused primarily on three Wi-Fi security issues: (1) data encryption, (2) authentication and access control, and (3) intrusion detection. While this debate has driven the Wi-Fi industry to rapidly improve security standards in each of these areas, security specialists have largely failed to address a critically important fourth component of WLAN security: wireless network management. Network management and network security are not separate issues that can be addressed in isolation. They are two sides of the same coin: if a Wi-Fi network is not managed, it cannot be secure.

## Wi-Fi Security: The Basic Requirements

Any organization planning a wireless network must have a strategy for addressing each of these critical areas of wireless LAN security:

### 1) Data Encryption

In a secure wireless network, the most obvious requirement is that all data transmitted between wireless client devices and wireless access points must be encrypted to prevent intruders from viewing the data.

### 2) Authentication & Access Control

The second absolute requirement of a secure wireless network is that only authorized, authenticated users should be able to connect to the network.

### 3) Intrusion Detection

Organizations must have an intrusion detection strategy that encompasses not just the detection of unauthorized network users but also location unauthorized wireless network devices (access points) connected to the network

### 4) Wireless Network Management

To implement a secure wireless network, the enterprise must define security policies and ensure that these policies are implemented uniformly across the entire network infrastructure.

The organization must continuously audit the infrastructure to ensure that these policies remain in effect at all times. If this is not done, the enterprise must assume that its wireless network is not secure.

## Wireless Data Encryption

Early Wi-Fi networks relied on the Wired Equivalent Privacy (WEP) standard, which uses a flawed security algorithm that provides a single security "key" for all users. This proved relatively easy to crack. As a result, early enterprise adopters of Wi-Fi technology often required their wireless users to connect to the WLAN using a VPN or proprietary client for encryption rather than relying on WEP alone.

To address the shortcomings of WEP, the Wi-Fi industry introduced a new standard known as Wi-Fi Protected Access (WPA). WPA uses longer 128-bit encryption keys and utilizes TKIP (Temporal Key Integrity Protocol) to provide unique encryption keys for each user and session. As a result, WPA provides much stronger data encryption than WEP and is being adopted rapidly by many enterprises. The primary barriers to WPA adoption are that it requires all client devices and access points to support the WPA standard and for the appropriate settings to be enabled on each of those devices. While most devices sold in recent years are WPA-compliant, legacy devices remain in most organizations today.

To address this timing issue, many organizations are using multiple VLANs on their wireless networks. One VLAN is for users with WPA-enabled devices while other users are segmented on an "untrusted" VLAN which has limited network access privileges and often forces users through a VPN or firewall.

To provide even more secure data encryption, the Wi-Fi industry has ratified the WPA2 (802.11i) standard, which uses an even stronger encryption algorithm known as AES. While WPA2-compliant products are now available on the market, few enterprises have yet adopted WPA2 since it also requires older client devices and access points to be updated with new software or replaced outright. In many cases, legacy Wi-Fi hardware may have to be replaced entirely to convert to WPA2 since the computational requirements of AES encryption are relatively high. As a result, enterprise conversion to WPA2 will likely be a very gradual process.

Still, most enterprises are planning to implement WPA2 at some point in the future and are starting to specify that all new APs and client devices be WPA-2 compliant to facilitate this transition.

## Authentication and Access Control

Most enterprises are migrating to 802.1x port-based authentication and access control solutions for their wireless networks. In an 802.1x authentication framework, every port is protected and each network user is verified through an authentication server, usually RADIUS. 802.1x was originally developed with wired network security in mind, but has been too costly to implement on wired networks because organizations would have to replace many of their existing switches with 802.1x-compliant switches. Ironically, since all enterprise-grade wireless APs support the 802.1x framework, 802.1x is being adopted much more rapidly for wireless network security than on the wired network. For example, both WPA and WPA2 rely on 802.1x and Extensible Authentication Protocol (EAP) for authentication.

Most enterprise IT organizations are already familiar and comfortable with the 802.1x framework. The primary barrier to its adoption is the requirement that all client devices and access points have the appropriate settings and firmware. There are many different EAP variants (PEAP, LEAP, WPA, WPA2, etc.). Organizations using the 802.1x framework must set a policy and ensure that the EAP variant they select is uniformly supported on all their clients and APs. As organizations transition, many are using the same type of 'multiple VLAN' strategy they are using to migrate from WEP to WPA or WPA2 (see above). Once again, these organizations use two or more VLANs on their wireless networks: a secure one for 802.1x/EAP-enabled devices and a separate VLAN for other devices.

The organizations experiencing the greatest difficulty migrating to the 802.1x framework are:

- Retailers and manufacturers using legacy or non-Windows-based handheld devices that do not support 802.1x.
- Colleges and universities with a wide variety of client devices with non-standard configurations.
- Wireless internet service providers (WISPs) who must support a wide variety of users' client devices.

Where it has not been feasible to implement 802.1x port-based authentication, organizations have adopted other means to secure their wireless networks, including wireless gateways, access control lists (ACLs), and various remote access control solutions like VPNs and firewalls.

Because wireless gateways provide access control without requiring specific client configurations, they are particularly useful in environments where there are many different types of client devices or where the IT organization does not have full control over clients (such as in the university and WISP markets). However, proprietary gateways can be expensive and difficult to manage when deployed in large numbers, making them a costly access control solution for most enterprises.

MAC-based access control lists are often used in environments with large numbers of legacy client devices without sufficient 'intelligence' for robust encryption and where cost is a major factor. In these instances, the access point is configured to permit only a predefined list of end devices (identified by MAC address) to connect to the network. While inexpensive to deploy, ACLs are susceptible to MAC spoofing and can be hacked without great difficulty. As a result, they are typically not used in high-security environments.

In other environments, VPNs and firewalls are still required to provide extremely high levels of security. Since most organizations have these solutions in place today, they can leverage their existing investment in security on the wireless network. However, since most VPNs were designed to support remote users only, as the wireless network expands and the user base grows these systems can be stretched beyond their limits, forcing IT to consider costly updates as the WLAN scales.

While organizations today may adopt different approaches to access control and authentication, there is growing momentum to adopt 802.1x-based solutions for secure, scalable wireless LAN roll-outs. No matter what policy is adopted, however, it is critical for the organization to define those policies centrally and ensure they are enforced uniformly across the network.

## Intrusion Detection

In traditional wired networks, the primary function of an intrusion detection system is to determine whether unauthorized *users* have connected to the network. Since

wireless LANs are typically installed as extensions of the existing Ethernet infrastructure, these same solutions can usually be leveraged effectively to identify unauthorized users of the wireless network. However, wireless networks introduce a significant new intrusion risk: IT must not only worry about unauthorized users, but also about the possibility that unauthorized network *equipment* will be connected directly to their network.

In the past, the cost, complexity, and size of wired Ethernet network equipment meant that it was practically unheard of for an employee or intruder to connect an unauthorized switch or router to the corporate network. If they did, detecting and locating the equipment would be relatively easy. With the rise of wireless LANs, however, this is no longer the case. Wi-Fi access points are inexpensive, portable, and easily available to the general public. They can quickly be connected to the network and can be difficult to detect with conventional tools. As a result, it is now essential that enterprises have an intrusion detection strategy to combat this new threat by detecting any unauthorized, unsecured wireless access points.

Whether deployed by well-meaning employees or malicious intruders, rogue access points provide an open window into the enterprise network. There are two primary methods through which rogue APs can be detected on the network:

- Wired Network Scans designed to identify rogues from the wired side of the network to which they are connected; and
- Wireless Scans using authorized wireless devices to detect the RF signal being broadcast by the rogue access points.

Ideally, organizations should use a combination of wired and wireless network scans to gather as much information as possible about rogue access points and to locate them on the network. As always, the appropriate intrusion detection solution for any organization will be determined by a combination of requirements, time, and budget.

### Wired Network Scans

Because few (if any) organizations have wall-to-wall wireless coverage via authorized APs or sensors, wired network scans represent the baseline intrusion detection that must be used by every organization.

Enterprise-grade wireless intrusion detection systems like the AirWave Management Platform™ conduct wireline scans in two ways:

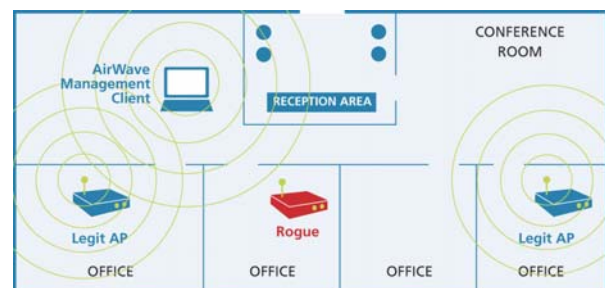
(1) "Fingerprinting" known makes and models of wireless access points so they can be detected automatically as soon as they are connected to the network. It is particularly important to detect the SOHO access points that are rarely used in authorized enterprise deployments but are the most common rogue APs. The AirWave Management Platform automatically identifies the fingerprints of more than 70 makes and models of AP.

(2) Interrogating routers and switches to identify every device connected to the network and assign each device a 'score' based on the likelihood of it being an unauthorized AP.

Wireline scans provide a great deal of information about the rogue device (such as the switch port to which the device is connected, the IP address of the device, etc.) that can be used to pinpoint the location of the device on the network.

### Wireless Network Scans

Wireless scans are a particularly effective means to detect rogue APs, because any functioning access point (including rogues) broadcasts an RF signal that can be detected wirelessly. Because wireless scans detect this RF signal,, they are highly accurate and have a very low rate of 'false positive' identifications. The greatest limitation of wireless scans is that a sensor device (an authorized AP, client device, or dedicated hardware probe) must be within a few hundred feet of the rogue in order to detect it.



The most cost-effective way to conduct wireless scans is typically to use existing, authorized access points to 'listen' for other unknown APs and ad hoc networks within range. The AirWave Management Platform can remotely instruct most enterprise-grade APs to conduct this type of wireless scan and to report the results. AMP then compares the list discovered

APs to its database of authorized access points to identify potential rogues. RF scanning via existing access points is very cost-effective because it requires no new or proprietary hardware. The primary limitation of this methodology is that only rogue APs within range of authorized APs can be discovered. The combination of AP-based wireless scans with wireline detection techniques and client-based wireless scans (see below) helps address this limitation.

Similarly, with appropriate software, WiFi-enabled client devices can also be used to report RF activity within range. The AirWave Management Client™ software, for example, enables Windows-based client devices to report all the APs within range. AMP then determines which of the detected APs are authorized and which are potential rogues. In this way, client devices can help fill coverage gaps where there is no wall-to-wall RF signal from existing APs.

Organizations with stringent security requirements and large capital budgets may consider using wireless IDS systems based on proprietary RF probes in addition to wireline scans and wireless detection via authorized APs and clients. While requiring costly hardware to be installed in all covered locations, these wireless IDS systems gather robust RF data that enable them to detect rogue APs, unauthorized client devices, man-in-the-middle attacks, denial-of-service attacks, and more.

## Wireless Network Management

A robust, comprehensive Wi-Fi management solution like the AirWave Management Platform™ is the final element of a secure wireless security architecture. To safeguard a wireless network, a management solution must give administrators total control over the network infrastructure.

### Network Discovery

A wireless LAN management solution must first automatically discover all wireless access points and other Wi-Fi devices connected to the wireless LAN infrastructure to ensure that network administrators have authorized each of these devices. To ensure discovery of all APs, the management solution must use a combination of Layer 2 discovery protocols (such as CDP, OSU NMS, WNMP, etc) as well as SNMP and HTTP network scans.

Once all APs have been discovered, the management solution must then generate accurate inventory reports for the IT staff to use to ensure (1) that no unknown devices have been

connected to the network and (2) they can account for all previously installed devices.

### Automated Configuration

Implementing secure encryption and access control on a wireless network requires that (1) the organization has defined centralized configuration policies, and (2) these policies are applied uniformly to all wireless APs and other devices. For example, if an organization specifies a security policy based on WPA with PSK, then every AP must have all the appropriate WPA settings enabled. If this organization is also using separate VLANs and/or SSIDs for different classes of network users (i.e., employees vs. guests), then these specific settings must also be applied correctly to each AP on the network.

**“Through 2006, 70% of successful WLAN attacks will occur because of misconfigured access points or client software.”**

Gartner Group (August 2004)

Configuring these settings manually creates numerous opportunities for human error that could jeopardize security. The Gartner Group has estimated that up to 70% of wireless LAN attacks will be the result of misconfigured APs and devices. The only way to provide true WLAN security is to use a solution like the AirWave Management Platform that automatically configures network hardware from all leading vendors.

Good network security also requires that passwords, SSIDs and other key security settings be rotated on a frequent basis. Without a centralized management solution that makes such configuration changes quickly and efficiently, best security practices are unlikely to be followed because of the labor required to manage settings on thousands of devices.

An efficient configuration solution is also essential when a wireless network is under attack. With a centralized solution like AMP, remote administrators can immediately shut down entire segments of the wireless network during an attack. They can even help avert attacks by scheduling the entire wireless network to shut down after hours, when there are no legitimate business users of the wireless network – and schedule the network to turn on once again at the start of business the next day.

### Audit Management

It is not enough to configure wireless APs and infrastructure devices correctly once, at the time of installation. Especially in large organizations with multiple IT staff members, it is extremely common for an access point to become misconfigured during trouble-shooting or due to human error. Worst case, if a malicious intruder connects to an AP's physical interface, he or she may be able to alter the configuration in a way that undermines all security policies put in place.

To combat misconfigured APs, wireless network management solutions must provide a detailed audit trail and system log to track each configuration change by user. By tracing the source of all configuration changes and errors, AMP ensures accountability and helps IT ensure that any staff members who cause configuration errors are better trained in the future.

In addition to providing accountability and training, organizations must conduct frequent audits of the configuration of each AP to ensure that its actual configuration always conforms to security policies. These audits simply cannot be conducted manually, since there can be hundreds of settings that must be checked on each wireless access point. Only a centralized management solution like AMP can quickly compare actual AP configurations to pre-defined policies, and automatically report any discrepancies. AMP uses a highly efficient process for polling devices and assessing their current configurations, enabling it to conduct audits on a continuous basis. Administrators can even set up the AirWave Management Platform to 'auto-repair' any configuration mismatches to ensure that all APs conform to network policies at all times.

In this way, a wireless network management solution can eliminate the risk that misconfigured access points will expose the network to attack.

### Firmware Management

An efficient solution for updating the software on access points and other network devices is a requirement for WLAN security. First, as hardware vendors identify and release patches to

address security vulnerabilities in their devices, it is essential for the organization to be able to distribute these updates efficiently to hundreds or even thousands of devices. Second, as organizations migrate to new security standards like WPA and WPA2, many of their legacy access points and devices will need to receive firmware updates to support these standards.

The AirWave Management Platform gives IT staff the ability to specify minimum acceptable firmware versions for each make and model of access point on the network. AMP contains an integrated TFTP server that allows it to automatically schedule and deliver these firmware updates after hours to avoid disrupting network performance.

### Network Monitoring & Alerting

A real-time monitoring solution that tracks each user by username is a critically important component of network security. Using real-time monitoring views, administrators can determine exactly who is connected to the network, where they are connected, whether they have been authenticated, and more. If unauthorized users have associated to a wireless access point but have not been authenticated onto the network, a monitoring system can help IT pinpoint identify these users, determine where they are connected to the network, and assess whether they are authorized users experiencing authentication problems or unauthorized users being blocked.

A monitoring solution can quickly alert IT when current usage patterns diverge significantly from expected, historical patterns, indicating the possibility of a security breach or other network problem. For example, the AirWave Management Platform can be configured to generate automated alerts when cumulative bandwidth through an AP exceeds a set threshold, as in a denial of service attack. Similarly, AMP may be programmed to generate an alert if the number of users connected to an AP in a warehouse or distribution facility exceeds the number of authorized devices or if the bandwidth being used by an individual device exceeds the threshold required for the supported applications in that facility. AMP's monitoring screens and reports even enable IT to view a detailed roaming and connection log for each user, tracking every session on the wireless network for both security and planning purposes.

## Conclusion

Without a wireless network management solution, it is virtually impossible to secure a large WLAN. Without a management solution in place, other steps taken to secure the Wi-Fi network are incomplete and ineffective:

- An organization may require strong encryption settings to protect data transmitted over the wireless network. Without a management solution, however, it is extremely difficult for the organization to ensure that these settings are applied uniformly on all network devices. Without this assurance, the organization cannot be sure that its data is protected.
- The enterprise may specify access control policies designed to ensure that only authorized users are permitted to connect to the corporate network. If the organization cannot guarantee that all wireless devices, RADIUS servers, and other network infrastructure are configured to conform with these policies, the organization runs the risk that unauthorized users will connect directly to their network wirelessly.
- For an intrusion detection solution to differentiate between authorized and unauthorized devices and users, it must first have a full and accurate inventory of all the authorized devices on the network.

Defining policies. Configuring devices. Auditing configuration settings. Maintaining accurate inventories. All of these are management tasks that must be performed routinely and reliably for a wireless network to be secure. The information security team at any organization deploying a wireless LAN must insist on a comprehensive management solution like the AirWave Management Platform. Without it, they cannot do their jobs and cannot guarantee the security of the organization's secure network resources.

---

### 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