# Cisco Aironet Wireless LAN Security Overview

## Why Wireless LANs?

Wireless local area networks (wireless LANs, or WLANs) are changing the landscape of computer networking. The use of mobile computing devices, such as laptops and personal digital assistants, coupled with the demand for continual network connections without having to "plug in," are driving the adoption of enterprise WLANs.

Organizations around the world are installing overlay WLANs and freestanding, all-wireless networks to increase employee productivity. In November 2001, an independent study by NOP World—one of the world's largest research and business information companies—found that WLANs enabled end users to stay connected an additional 1.75 hours each day, resulting in an increase in productivity of up to 22 percent.

Network managers are using WLANs to facilitate network moves, adds and changes. In addition, the inherent flexibility of WLANs overcomes limitations created by older buildings, leased spaces, or temporary work areas.

A WLAN allows end users to access e-mail, schedule meetings, and access files and applications on the corporate or university network from conference rooms, classrooms, coworkers' desks, and virtually anywhere on campus. With wireless networking, regardless of where they are in a facility, end users are just a mouse-click away from key information and applications.

## WLAN Security Concerns

With the increased reliance on WLANs, businesses are increasingly more concerned about network security. Network managers need to provide end users with freedom and mobility without offering intruders access to the WLAN or the information sent and received on the wireless network.

With a WLAN, transmitted data is broadcast over the air using radio waves. This means that any WLAN client within an access point (AP) service area can receive data transmitted to or from the access point. Because radio waves travel through ceilings, floors, and walls, transmitted data may reach unintended recipients on different floors or even outside the building that houses the AP. With a WLAN, the boundary for the network has moved. Without stringent security measures in place, installing a WLAN can be the equivalent of putting Ethernet ports everywhere, including the parking lot.

Because of these security concerns, many network managers have been reluctant or unwilling to deploy WLANs, especially in light of the vulnerability of the Wired Equivalent Privacy (WEP) keys that are used to encrypt and decrypt transmitted data. Several research papers and articles have highlighted the potential vulnerabilities of static WEP keys. In addition, hackers have ready access to tools for cracking WEP keys, such as AirSnort, which enables an attacker to passively monitor and analyze packets of data and then use this information to break the WEP key that encrypts the packets. Network managers need reassurance that WLANs can provide the same level of security, manageability, and scalability offered by wired LANs.

## Turning on WLAN Security

To mitigate threats to a WLAN, network managers need to deploy several layers of defense across the network. Securing a WLAN is just one component of the overall enterprise security framework. Other components, including firewalls, intrusion-detection systems, and segmented networks, should be considered as part of the network design in addition to WLAN security.

Network managers must also *turn on* their WLAN security features. A recent *Wall Street Journal* article described two hackers with a laptop and a boom antenna who drove around Silicon Valley, sniffing for stray WLAN signals. The hackers were able to pick up signals from numerous companies that had not turned on their WLAN security features.

Cisco recommends that all organizations that use WLANs turn on their WLAN security features. Cisco further recommends that an organization perform network risk assessments before selecting and implementing a WLAN security solution.

## Traditional WLAN Security

As with other networks, security for WLANs focuses on access control and privacy. Robust WLAN access control prevents unauthorized users from communicating through APs, the WLAN endpoints on the Ethernet network that link WLAN clients to the network. Strong WLAN access control ensures that legitimate clients associate with trusted, rather than “rogue” APs. WLAN privacy ensures that only the intended audience understands the transmitted data. The privacy of transmitted WLAN data is protected only when that data is encrypted with a key that can be used only by the intended recipient of the data.

Traditional WLAN security includes the use of Service Set Identifiers (SSIDs), open or shared-key authentication, static WEP keys and optional Media Access Control (MAC) authentication. This combination offers a rudimentary level of access control and privacy, but each element can be compromised.

An SSID is a common network name for the devices in a WLAN subsystem; it serves to logically segment that subsystem. An SSID prevents access by any client device that does not have the SSID. By default, however, an AP broadcasts its SSID in its beacon. Even if broadcasting of the SSID is turned off, an intruder or hacker can detect the SSID through sniffing.

The 802.11 standard, a group of specifications for WLANs created by the Institute of Electrical and Electronics Engineers Inc. (IEEE), supports two means of client authentication: open and shared-key authentication. Open authentication involves little more than supplying the correct SSID. With shared-key authentication, the AP sends the client device a challenge text packet that the client must then encrypt with the correct WEP key and return to the access point. If the client has the wrong key or no key, authentication will fail and the client will not be allowed to associate with the access point. Shared-key authentication is not considered secure, because a hacker who detects both the clear-text challenge and the same challenge encrypted with a WEP key can decipher the WEP key.

With open authentication, even if a client can complete authentication and associate with an AP, the use of WEP prevents the client from sending data to and receiving data from the AP, unless the client has the correct WEP key.

Another type of key that is often used, but is not considered secure, is a “static” WEP key. A static WEP key is a key composed of either 40 or 128 bits that is statically defined by the network administrator on the AP and all clients that communicate with the AP. When static WEP keys are used, a network administrator must perform the time-consuming task of entering the same keys on every device in the WLAN.

If a device that uses static WEP keys is lost or stolen, the possessor of the stolen device can access the WLAN. An administrator won’t be able to detect that an unauthorized user has infiltrated the WLAN, until and unless the theft is reported. The administrator must then change the WEP key on every device that uses the same static WEP key used by the missing device. In a large enterprise WLAN with hundreds or even thousands of users, this can be a daunting task. Worse still, if a static WEP key is deciphered through a tool like AirSnort, the administrator has no way of knowing that the key has been compromised by a hacker.

Some WLAN vendors support authentication based on the physical address, or MAC address, of the client Network Interface Card (NIC). An access point will allow association by a client only if that client's MAC address matches an address in an authentication table used by the access point. But MAC authentication is an inadequate security measure, because MAC addresses can be forged, or a NIC can be lost or stolen.

While traditional WLAN security that relies on SSIDs, open or shared-keys, static WEP keys or MAC authentication is better than no security at all, it is not sufficient for the enterprise organization. Only very small businesses, or those that do not entrust mission-critical data to their WLAN networks, can rely on these WLAN security types. All other enterprises and organizations must invest in a robust, enterprise-class WLAN security solution.

## Cisco Wireless Security Suite Advantage

Today’s corporate WLANs need secure, business-class protection and manageability. A secure WLAN solution must address the following areas:

- 802.11 standards
- 802.1X authentication standards
- WEP key management
- User and session authentication
- Access point authentication
- Detection of rogue access points
- Unicast key management
- Client session accounting records
- Mitigation of network attacks
- WLAN management
- Operating system support

The Cisco Wireless Security Suite for the Cisco Aironet® Series provides robust wireless security services that closely parallel the security available in a wired LAN. The Cisco Wireless Security Suite provides network managers with an enterprise-class solution that offers freedom and mobility to end users while maintaining a secure network environment.

The Cisco Wireless Security Suite solution fulfills the need for a consistent, reliable, and secure mobile networking solution. This 802.1X-based solution provides scalable, centralized security management and supports dynamic per-user, per-session WEP encryption keys to protect the privacy of transmitted data. Other features include mutual authentication, message integrity check, and per-packet keying to ensure that every data packet is encrypted with a different key.

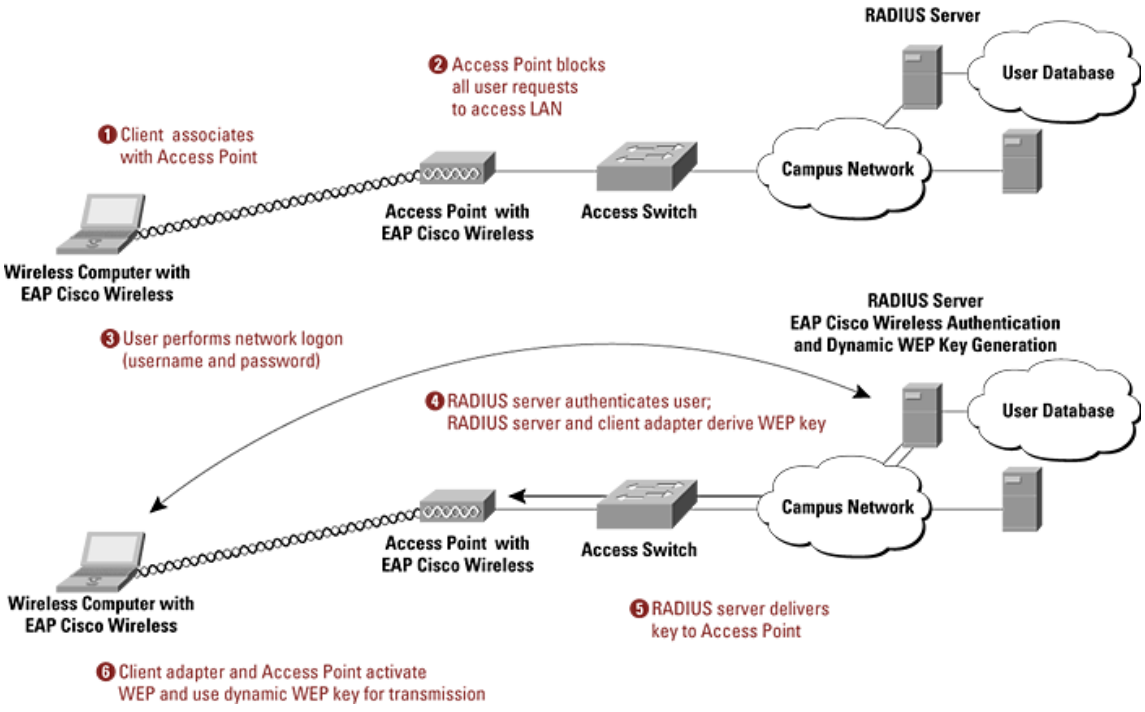
## 802.1X Authentication

The IEEE has adopted 802.1X as a new standard for authentication on wired and wireless networks. This standard provides WLANs with strong, mutual authentication between a client and an authentication server. In addition, 802.1X can provide dynamic per-user, per-session WEP keys, removing the administrative burden and security issues surrounding static WEP keys.

Several 802.1X authentication types exist, each providing a different approach to authentication while relying on the same framework and the Extensible Authentication Protocol (EAP) for communication between a client and an AP.

Cisco has developed an 802.1X authentication type called EAP Cisco Wireless, or Cisco LEAP. Cisco LEAP is part of the Cisco Wireless Security Suite. Cisco Aironet products support Cisco LEAP and all 802.1X authentication types, including EAP Transport Layer Security (EAP-TLS). With 802.1X authentication types such as Cisco LEAP and EAP-TLS, mutual authentication is implemented between the client and a Remote Authentication Dial-In User Service (RADIUS) server. The credentials used for authentication, such as a log-on password, are never transmitted in the clear, or without encryption, over the wireless medium.

Figure 1 EAP Cisco Wireless (Cisco LEAP) Mutual Authentication



With traditional WLAN security, anyone with a device that is part of the WLAN network is in possession of the client device's MAC address and the static WEP key. If a device is lost or stolen, the client card and MAC address can be used to gain access to the WLAN—without detection. The use of an 802.1X authentication type like Cisco LEAP, which authenticates a client by asking for a password, to be supplied by the user, rather than performing an authentication based on a physical attribute of the client device, minimizes the risks associated with the loss of a device or its WLAN NIC.

### Man-In-The-Middle Authentication Attacks

A WLAN man-in-the-middle authentication attack is a network attack in which a network intruder intercepts authentication messages between the client and AP to gain access to the network. This is an active attack using packet sniffers.

The possible consequences of such an attack includes theft of information, hijacking of an ongoing session to gain access to internal network resources, traffic analysis to derive information about a network and its users, denial of service, corruption of transmitted data, and introduction of new information into network sessions.

Mutual authentication with 802.1X mitigates potential man-in-the-middle authentication attacks by rouge APs and ensures that legitimate clients associate only with legitimate and authorized APs. Because traditional 802.11 and MAC authentication are one-way, rather than mutual, the client has no way to determine whether the AP from which it is receiving data is a "trusted" AP. If a client inadvertently associates and communicates with a rogue AP, the client is "hijacked" from the trusted network without the user's awareness. With mutual authentication, the client challenges the AP for credentials, which the AP can provide only if it is authorized to communicate with a trusted RADIUS server that has access to the credentials. A client device will not associate with any AP that cannot respond correctly to the client's challenge.

### Centralized WEP Key Management and Policy-Based Key Rotation

Another benefit of 802.1X authentication is centralized management of WEP keys. Once mutual authentication has been successfully completed, the client and RADIUS server each derive the same WEP key, which will be used to encrypt all data exchanged. Using a secure channel on the wired LAN, the RADIUS server sends the key to the AP, which stores it for the client. The result is per-user, per-session WEP keys, with the length of a session determined by a policy defined on the Cisco Secure Access Control Server (ACS), which is Windows-based, or the Cisco Access Registrar (AR) RADIUS server, which is UNIX-based. When a session expires or the client roams from one AP to another, a reauthentication occurs and generates a new session key. The reauthentication is transparent to the user.

### Brute-Force Attacks

Traditional WLAN implementations based on static WEP are easily susceptible to "brute-force" network attacks. A brute-force network attack is one in which the intruder attempts to derive a WEP key by trying one value at a time. For standard 128-bit WEP, this would require trying a maximum of $2^{104}$ different keys. The use of dynamic, per-user, per-session WEP keys makes a brute-force attack, although still theoretically possible, extremely difficult to conduct and virtually futile.

## Temporal Key Integrity Protocol WEP Key Enhancements

While 802.1X and EAP authentication types provide strong authentication for wireless LANs, standard 802.11 WEP encryption is still vulnerable to network attacks.

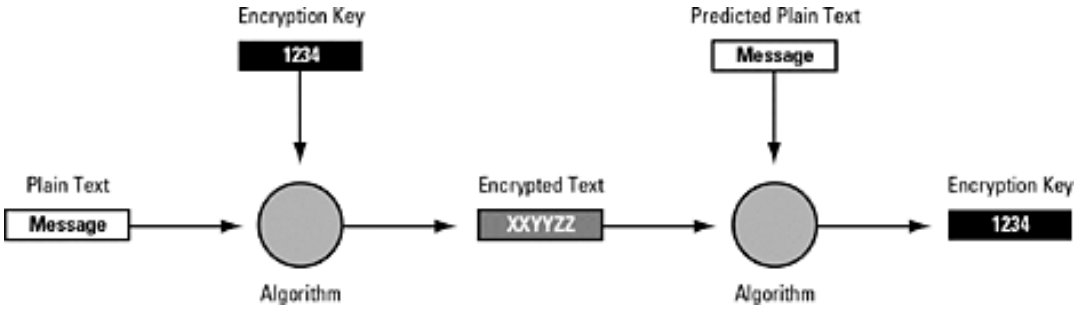
The Cisco Wireless Security Suite provides several enhancements to WEP keys, both static WEP keys and the dynamic keys that are derived as a result of a successful 802.1X authentication. These WEP enhancements include pre-standard Temporal Key Integrity Protocol (TKIP), support for Message Integrity Check (MIC), per-packet key hashing, and broadcast key rotation.

### Message Integrity Check Protection from Active Network Attacks

The use of a Message Integrity Check, or MIC, thwarts an active network attack designed to determine the WEP key used to encrypt intercepted packets. This active attack is a combination of a bit-flipping attack and a replay attack. The attack proceeds as follows:

- Hacker intercepts WEP-encrypted packet
- Hacker flips bits in packet and recalculates Integrity Check Value (ICV)
- Hacker transmits to AP bit-flipped frame with known initialization vector (IV)
- Because ICV is correct, AP accepts, forwards frame
- Layer 3 device rejects and sends predictable response
- AP encrypts response and sends it to hacker
- Hacker uses response to derive key (stream cipher)

Figure 2 Active Attack: When a hacker who receives an encrypted message knows the plain-text version of the message, then the hacker can determine the encryption key, or stream cipher, used to encrypt the message.




When MIC support is implemented on both the AP and all associated client devices, the transmitter of a packet adds a few bytes (the MIC) to the packet before encrypting and transmitting it. Upon receiving the packet, the recipient decrypts it and checks the MIC. If the MIC in the frame matches the calculated value (derived from the MIC function), the recipient accepts the packet; otherwise, the recipient discards the packet.

Using MIC, packets that have been (maliciously) modified in transit are dropped. Attackers cannot use bit-flipping or active replay attacks to fool the network into authenticating them, because Cisco Aironet products, which are MIC-enabled, identify and reject altered packets.

### Per-Packet Key Hashing to Mitigate "Weak IV" Attacks

When a WEP key is used to encrypt and decrypt transmitted data, each packet includes an initialization vector (IV), which is a 24-bit field that changes with each packet. The RC4 Key Scheduling Algorithm creates the IV from the base WEP key. A flaw in the WEP implementation of RC4 allows the creation of "weak" IVs that give insight into the base key. Using a tool like AirSnort, a hacker can exploit this flaw by gathering packets encrypted with the same key and using the weak IVs to calculate the base key.

The Cisco Wireless Security Suite supports a pre-standard version of TKIP, which includes key hashing, or per-packet keying. When key-hashing support is implemented on both the AP and all associated client devices, the transmitter of data hashes the base key with the IV to create a new key for each packet. By ensuring that every packet is encrypted with a different key, key hashing removes the predictability that an intruder relies on to determine the WEP key by exploiting IVs.

## Broadcast Key Rotation

The Cisco Wireless Security Suite allows network managers to rotate both the unicast keys and the broadcast WEP keys used to encrypt broadcasts and multicasts. Network managers configure broadcast-key rotation policies on the APs. Since a static broadcast key is susceptible to the same attacks as the unicast or static WEP keys, a key rotation value for broadcast keys is provided, which eliminates this susceptibility.

## WLAN Attacks and Mitigation Mechanisms

Table 1 outlines some of the most common WLAN attacks, as well as the mitigating mechanism and the effectiveness of each mitigation against the attack. As detailed in Table 1, static WEP is the most vulnerable to all of the listed attacks. Cisco LEAP, combined with WEP, does mitigate authentication attacks by using mutual authentication; however, the Cisco LEAP/WEP combination, when used without the other security components in the Cisco Wireless Security Suite, is vulnerable to Man-In-The-Middle, and Fluhrer AirSnort WEP attacks. EAP-TLS, with its digital certificates, mitigates authentication forging, rogue access points and dictionary attacks.

On the far right, the Cisco Wireless Security Suite is shown to mitigate all of the listed attacks—with only a slight vulnerability to dictionary attacks, which can be mitigated by the use of strong passwords.

Table 1 WLAN Attack Mitigation Chart

| | | | | Cisco Wireless Security Suite |
|---|---|---|---|---|
| **Attack** | **Static WEP** | **Cisco LEAP and WEP** | **EAP-TLS** | **Cisco LEAP, TKIP, Broadcast Key Rotation, MAC Authorization, and Per-packet Keying** |
| **Man-In-The-Middle** | Vulnerable | Vulnerable | Vulnerable | Mitigated |
| **Authentication Forging** | Vulnerable | Mitigated | Mitigated | Mitigated |
| **Fluhrer (FMS Paper)** | Vulnerable | Vulnerable | Vulnerable | Mitigated |
| **Rogue Access Points** | Vulnerable | Mitigated | Mitigated | Mitgated |
| **Dictionary Attacks[1]** | Vulnerable | Mitigated[2] | Mitigated | Mitigated[2] |

1. A dictionary attack is a brute force method of compromising network security. During a dictionary attack, a network intruder uses a list of know passwords in various combinations to try to access the network via a known user's account. The intruder uses weak user passwords or words that are found in the dictionary during this attack

2. Requires Strong Passwords

## Managing Secure WLANs

Network managers are pressed for time. A WLAN solution needs to provide hassle-free security administration that does not increase the burden on the IT staff. WLAN security needs to be easy to install, manage, audit and update. The Cisco Wireless Security Suite includes several enhancements that simplify WLAN management and security, including the Cisco Wireless Utility Auto Installer, third-party AAA RADIUS server support, and the ability to generate detailed RADIUS accounting records.

### Hassle-Free Security

The Cisco Wireless Security Suite provides hassle-free security administration that does not increase the administrative burden on the IT staff. The Cisco Wireless Security Suite solution is flexible enough to allow network managers to choose the appropriate level of protection, yet robust enough to provide a framework around which a total security solution can be built. With the Cisco Wireless Security Suite, network administrators do not need to manage static WEP keys. They can also program their WLANs to require reauthentication as often as is necessary for their networks.

The Cisco Wireless Security Suite also provides operating system support for Microsoft Windows 95, 98, NT, 2000, Me, and XP, Mac OS, Linux and Windows CE. Read more about easily configuring Cisco APs in the Cisco Application Note: Configuring the Cisco Wireless Security Suite.

### Secure Automated Client Updates and Web Management

The Cisco Wireless Utility Auto Installer saves network administrators time by automatically and securely installing and upgrading Cisco Aironet client utilities, firmware, and user profiles, including security settings, SSIDs, power settings, and channel selection.

Support for Cisco Discovery Protocol (CDP) for auto-discovery of Cisco Aironet APs and bridges using Cisco enterprise management applications such as CiscoWorks2000 is provided. Web-based management and Simple Network Management Protocol (SNMP) features are also available to aid monitoring, troubleshooting, software downloads, and even logging. APs are installed quickly and accurately with help from the Cisco Site Survey Tool (SST), integrated into the client utility.

### Third-Party AAA RADIUS Support

Several third-party AAA RADIUS servers including Funk Software (Steel-Belted RADIUS) and Interlink Networks (AAA RADIUS) now support the Cisco LEAP security framework. These servers, along with the Cisco Secure Access Control Server (ACS) and Cisco Access Registrar (AR), provide network managers with flexibility and options for selecting back-end services without compromising WLAN security.

### RADIUS Accounting Records

With the Cisco Wireless Security Suite, detailed RADIUS accounting records for each client session can be generated. These records can be sent to AAA servers for recording, auditing, and billing for WLAN usage. Enterprises can also use these records to debug their networks.

## Specialized Wireless LAN Security

A specialized security solution using Virtual Private Network (VPN) is also available for companies that may require end-to-end WLAN security to protect their business applications. Most enterprise customers do not need to implement a specialized security WLAN within their intranets, but a select few, such as financial institutions, which require extensive security measures, may implement the specialized solution in conjunction with enhanced security. Additional information about using VPN for WLANs is available in the white paper *SAFE: Wireless LAN Security in Depth*.

For the vast majority of enterprise networks, an enhanced security solution, such as the Cisco Wireless Security Suite, meets and exceeds their WLAN security needs. The additional overhead and expense of a WLAN with VPN is not always necessary.

## Summary

With the Cisco Wireless Security Suite security features properly configured and activated, network administrators can feel confident that their company data will remain private and secure. Network managers can give their end-users freedom and mobility without offering that same freedom to hackers. With Cisco Aironet products, enterprise employees are wireless, secure, and ready to work.

Read more about WLAN security at the Cisco Wireless LAN Security Web site.


Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems Europe
11 Rue Camille Desmoulins
92782 Issy-les-Moulineaux
Cedex 9
France
www-europe.cisco.com
Tel: 33 1 58 04 60 00
Fax: 33 1 58 04 61 00

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 317 7777
Fax: +65 317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the

**Cisco Web site at www.cisco.com/go/offices**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland
Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland
Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden
Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe



06/02 BW8360