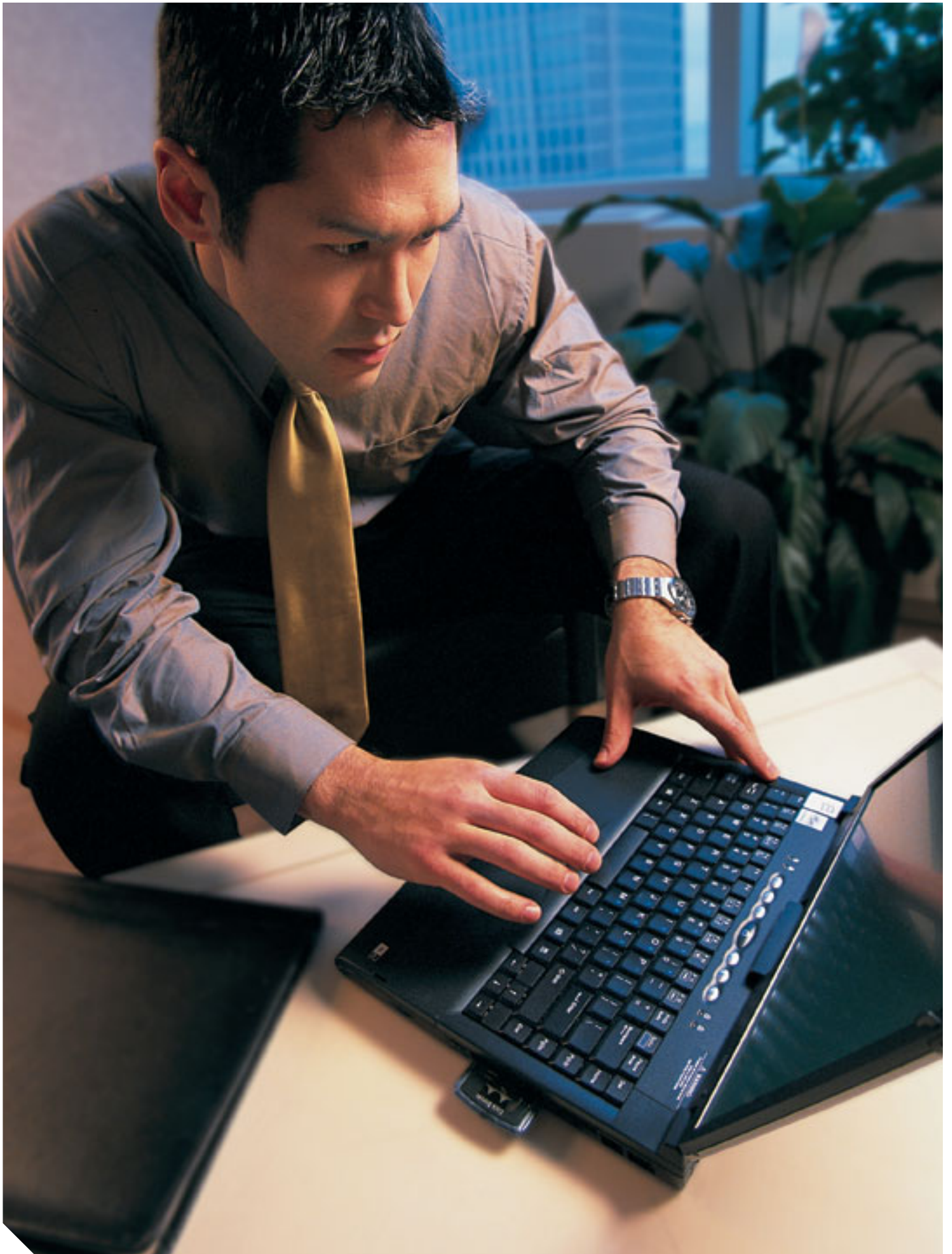


Cisco Aironet Wireless LAN Security



Give your network users
freedom and mobility
without giving up network security.





The Cisco Aironet Series— wireless freedom with enterprise-class security.

Perhaps the only thing more important to your business than the data exchanged on your network is the ability to maintain the security of that data. Security fears have caused some network managers to avoid installing wireless LANs (WLANs), regardless of the numerous benefits that they provide.

Now the landscape of wireless security has changed, giving IT managers the confidence to deploy WLANs. Today there's the Cisco® Wireless Security Suite—an enterprise-ready, standards-based, WLAN security solution for Cisco Aironet® Series products and Cisco Compatible WLAN client devices.

Features of the Cisco Wireless Security Suite include:

- Strong, mutual authentication and dynamic encryption key management via support for IEEE 802.1X
- Data encryption using Temporal Key Integrity Protocol (TKIP), Wired Equivalent Privacy (WEP) and, in 2004, Advanced Encryption Standard (AES)
- Strong TKIP encryption enhancements such as message integrity check (MIC), per-packet keys via initialization vector hashing, and broadcast key rotation
- Support for the broadest range of 802.1X authentication types, client devices, and client operating systems on the market
- Mitigation of network attacks
- Full support for the Wi-Fi Alliance security standard Wi-Fi Protected Access (WPA), introduced in 2003

Cisco, the network leader and a driving force behind wireless networking, has made it possible for network managers to give users the freedom they crave without sacrificing the network security they demand.



Security to Keep Intruders Out

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 that travel between client devices, or stations, and access points—the WLAN endpoints on the Ethernet network that link stations to the network. This means that any WLAN client device within an access point 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 access point. 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 in the parking lot.

Additionally, several research papers and articles have highlighted the vulnerabilities of WEP keys used to encrypt and decrypt transmitted data. Intruders 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 solutions are available to protect their WLANs from these vulnerabilities and that WLANs can provide the same level of security, manageability, and scalability offered by wired LANs.

The Importance of Using WLAN Security

Just as in wired networks, no one can guarantee a completely secure networking environment that will prevent all penetrations at all times. Security protection is dynamic and ongoing—not static. Network managers and WLAN manufacturers need to keep one step ahead of the hackers.

Network managers must also *turn on* their WLAN security features. In 2001, an article in *The Wall Street Journal* described two hackers who drove around Silicon Valley with a laptop and a boom antenna “sniffing” for stray WLAN signals. The hackers were able to pick up signals from numerous companies that had simply not bothered to turn on the appropriate WLAN security features.

Security experts recommend that enterprises deploy several layers of defense across the network to mitigate threats. Additional security components might include firewalls, intrusion-detection systems (IDSs), and virtual LANs (VLANs). Network managers also reduce risk by wisely designing and installing their wireless networks, by implementing proven security measures, and by using products and software developed by experts in network security. As an industry leader in network security, Cisco is an excellent choice for WLAN implementation. With the award-winning security features of the Cisco Wireless Security Suite, network managers can decrease risks to their network and increase WLAN security.



After twelve months of extensive testing in a real-world lab environment, the editors of *Network Computing* awarded the Cisco Aironet 1200 Series the 2003 Well-Connected Award in the Enterprise WLAN System category. These networking experts found the Cisco Aironet 1200 Series to be a truly innovative solution that meets real-world enterprise networking needs.

Multiple plenum-rated Cisco Aironet access points, which are the center points in an all-wireless network or the connection points between a wired and wireless network, can be placed throughout a building or campus.

Cisco Aironet access points provide users equipped with Cisco or Cisco Compatible WLAN client adapters the ability to move freely about covered areas of the campus.

The Cisco Wireless Security Suite maintains fully secure, uninterrupted access to all network resources, and the Cisco Structured Wireless-Aware Network supports deployment, operation, and management of hundreds to thousands of Cisco Aironet access points.



Wireless LAN Security Solutions

As with other networks, security for WLANs focuses on access control and privacy. Robust WLAN access control, also called authentication, prevents unauthorized users from communicating through access points. Strong WLAN access control measures help ensure that legitimate client stations associate only with trusted access points rather than rogue or unauthorized access points.

WLAN privacy helps ensure that only the intended audience understands the transmitted data. The privacy of transmitted WLAN data is considered protected when that data is encrypted with a key that can be used only by the intended recipient of the data. Encrypting data helps ensure that it remains uncorrupted throughout the sending-and-receiving transmission process.

Today, companies using WLANs are employing four distinct WLAN security solutions to address WLAN access control and privacy: open access, basic security, enhanced security, and remote access security. As with any security deployment, Cisco recommends that an organization perform network risk assessments before selecting and implementing any WLAN security solution.

Open Access

All Wi-Fi certified wireless LAN products, such as Cisco Aironet Series products, are shipped in “open-access” mode, with their security features turned off. While open access or no security may be appropriate and acceptable for public hot spots such as coffee shops, college campuses, airports, or other public locations, it is not an option for an enterprise organization. Security needs to be enabled on wireless devices during their installation in enterprise environments. As mentioned previously, some companies are not turning on their WLAN security features. These companies are exposing their networks to serious risk.



Basic Security: SSIDs, WEP, and MAC Address Authentication

Basic 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.

“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 access point broadcasts its SSID in its beacon. Even if broadcasting of the SSID is turned off, an intruder or hacker can detect the SSID through what is known as “sniffing”—or undetected monitoring of the network.

The 802.11 standard, a group of specifications for WLANs created by the 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 access point 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. Without the correct 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 an intruder 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 access point, the use of WEP prevents the client from sending data to and receiving data from the access point, unless the client has the correct WEP key. A WEP key is composed of either 40 or 128 bits and usually is statically defined by the network administrator on the access point and all clients that communicate with the access point. 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, unless and until 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 such as AirSnort, the administrator has no way of knowing that the key has been compromised by an intruder.

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.

Basic Security with WPA Pre-Shared Key

Another form of basic security now available is WPA Pre-Shared Key (PSK). The PSK verifies users via a password, or identifying code, on both the client station and the access point. A client may only gain access to the network if the client's password matches the access point's password. The password also provides keying material that TKIP uses to generate an encryption key for each packet of transmitted data. While more secure than static WEP, WPA PSK is similar to static WEP in that the PSK is stored on the client station and can be compromised if the client station is lost or stolen. A strong PSK passphrase that uses a mixture of letters, numbers and non-alphanumeric characters is recommended.

Basic Security Summary

Basic WLAN security that relies on a combination of SSIDs, open authentication, static WEP keys, MAC authentication, or WPA PSK is sufficient only for very small businesses, or those that do not entrust mission-critical data to their WLAN networks. All other organizations must invest in a robust, enterprise-class WLAN security solution.

Enhanced Security—The Cisco Wireless Security Suite Advantage

Enhanced security is recommended for those customers requiring enterprise-class security. The Cisco Wireless Security Suite is an enhanced security solution that provides full support for WPA and its building blocks of 802.1X and TKIP. The following features are part of the Cisco Wireless Security Suite:

- 802.1X for strong, mutual authentication and dynamic per-user, per-session encryption keys
- TKIP for enhancements to RC4-based encryption such as key hashing (per-packet keying), message integrity check (MIC), initialization vector (IV) changes, and broadcast key rotation

Because it is an enhanced security solution, the Cisco Wireless Security Suite gives network administrators confidence that they are deploying WLANs with enterprise-class security and protection.

Remote Access Wireless LAN Security

In certain instances, enterprises may require end-to-end security to protect their business applications. With remote access security, administrators set up a virtual private network (VPN) to allow mobile users in public hot spots, such as airports, hotels, and convention centers, to tunnel back to the corporate network.

Some enterprises, such as financial institutions, which require extensive security measures, might also implement a VPN for WLANs within their intranets, in conjunction with enhanced security. However, an enhanced security solution, such as the Cisco Wireless Security Suite, meets and exceeds WLAN security requirements for the vast majority of enterprise networks. The additional overhead, limitations, and expense of a VPN overlay for an internal WLAN are not necessary.

Additional information about using VPN for WLANs or installing an enhanced WLAN security solution is available in the white paper: Cisco SAFE: Wireless LAN Security in Depth. SAFE Blueprints from Cisco are a modular approach to securing a WLAN network in which security design, implementation, and management processes are specified.

Peace of Mind with the Cisco Wireless Security Suite

In order to deploy large-scale enterprise WLANs, network administrators need scalable, problem-free security administration that does not increase the burden on the IT staff. With the Cisco Wireless Security Suite, administrators do not need to manage static encryption keys, and WLANs can be programmed to require reauthentication as often as is necessary.

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. This enterprise WLAN security solution integrates quality of service (QoS) and mobility into its framework to enable a rich set of enterprise applications.

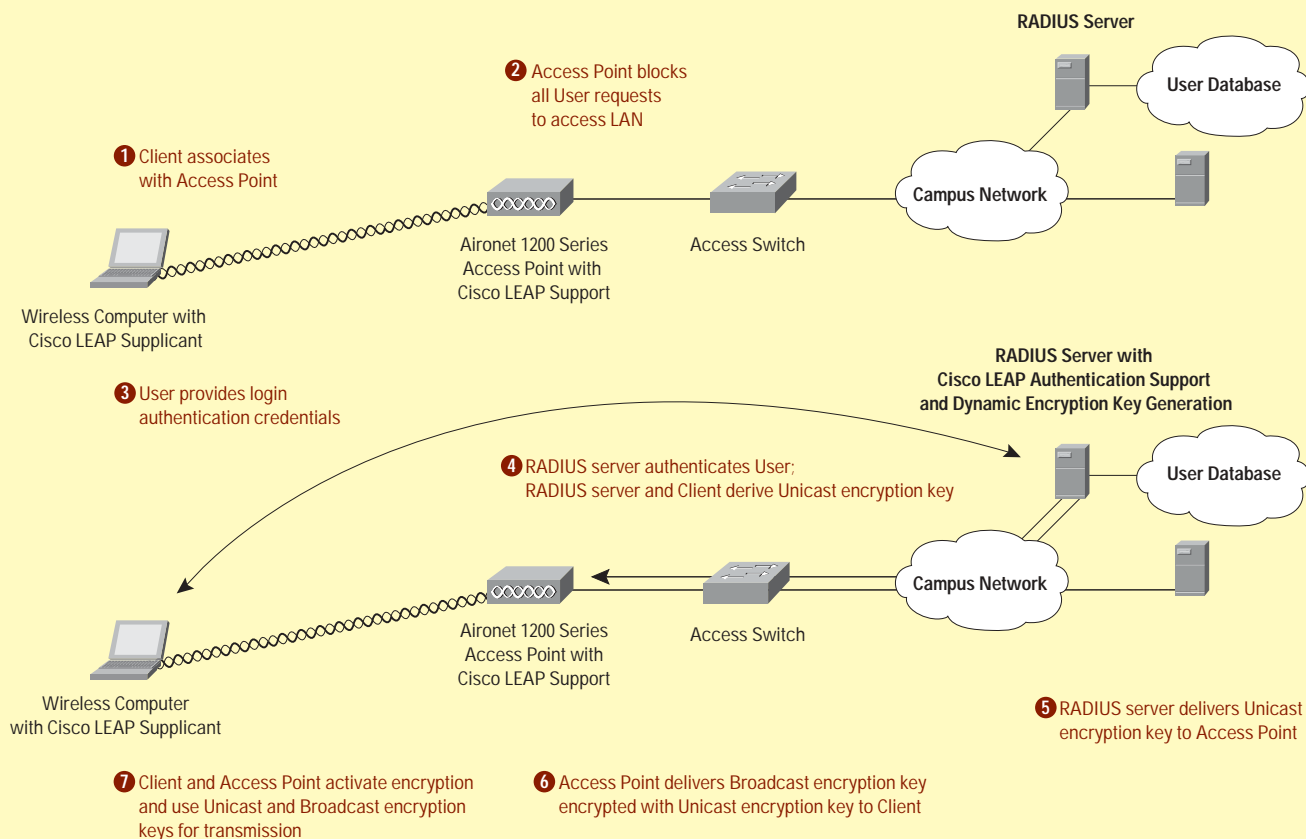
This enterprise-class solution mitigates sophisticated passive and active WLAN attacks and provides reliable, scalable, centralized security management with support for:

- Wi-Fi Protected Access (WPA)
- Cisco Structured Wireless-Aware Network (SWAN)
- Cisco Aironet access points and wireless LAN client adapters
- Cisco Compatible WLAN client devices

802.1X Authentication and the Extensible Authentication Protocol

The IEEE has adopted 802.1X as a 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 provides dynamic per-user, per-session encryption keys, removing the administrative burden and security issues surrounding static encryption keys. With 802.1X, the credentials used for authentication, such as logon passwords, are never transmitted in the clear, or without encryption, over the wireless medium.

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 access point. Cisco Aironet products support more 802.1X EAP authentication types than any other WLAN



products. Supported types include: Cisco LEAP, EAP-Transport Layer Security (EAP-TLS), and types that operate over EAP-TLS, such as Protected Extensible Authentication Protocol (PEAP), EAP-Tunneled TLS (EAP-TTLS), and EAP-Subscriber Identity Module (EAP-SIM).

Cisco recommends that customers evaluate their networks and security environments to select the best EAP authentication type for their 802.1X deployment. Areas to evaluate when selecting an EAP type include the type of security mechanism used for security credentials, the user authentication database, the client operating systems in use, the available client supplicants, the type of user login needed, and Remote Authentication Dial-In User Service (RADIUS) or Authentication, Authorization, and Accounting (AAA) servers.

Each EAP type has advantages and disadvantages. Trade-offs exist between the security provided, EAP type manageability, the operating systems supported, the client devices supported, the client software and authentication messaging overhead, certificate requirements, user ease of use and WLAN infrastructure device support. Multiple EAP types might also be used within a network to meet specific authentication, client device, or end user needs.

A wide selection of RADIUS servers, such as the Cisco Secure Access Control Server (ACS) and Cisco CNS Access Registrar,[®] or third-party AAA RADIUS servers, such as Funk Software (Steel-Belted RADIUS) and Interlink Networks (AAA RADIUS), can be used for 802.1X authentication.

The use of an 802.1X authentication type that authenticates a client station through user-supplied credentials rather than a physical attribute of the client device minimizes the risks associated with the loss of a device or its WLAN NIC. 802.1X provides other benefits, including mitigation of “man-in-the-middle” authentication attacks, centralized encryption key management with policy-based key rotation, and protection from “brute-force” attacks.

Centralized Policy Management for WLAN Users

Another benefit of 802.1X authentication is centralized management for WLAN user groups, including policy-based key rotation, dynamic key assignment, dynamic VLAN assignment, and SSID restriction. These features rotate the encryption keys. They also assign users to specific VLANs to ensure that users are only allowed access to specific resources.

After mutual authentication has been successfully completed, the client and RADIUS server each derive the same encryption key, which is used to encrypt all data exchanged. Using a secure channel on the wired LAN, the RADIUS server sends the key to the access point, which stores it for the client. The result is per-user, per-session encryption keys, with the length of a session determined by a policy defined on the RADIUS server. When a session expires or the client roams from one access point to another, a reauthentication occurs and generates a new session key. The reauthentication is transparent to the user.

In conjunction with encryption keys and the reauthentication timer, VLAN ID and SSID restriction parameters are passed to the access point. When the access point receives the VLAN ID assignment for a specific user, it places that user on the specified VLAN ID. If the allowed SSID list is also passed to the access point, the access point will help ensure that the user is providing a valid SSID ID to access the WLAN. If the user provides an SSID not specified in the allowed SSID list, the access point disassociates the user from the WLAN network.

Mitigation of Brute-Force Attacks

Traditional WLAN implementations based on static encryption keys are easily susceptible to “brute-force” network attacks. A brute-force network attack is one in which the intruder attempts to derive an encryption 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 802.1X dynamic, per-user, per-session encryption keys makes a brute-force attack, although still theoretically possible, extremely difficult to conduct and virtually futile.

Temporal Key Integrity Protocol

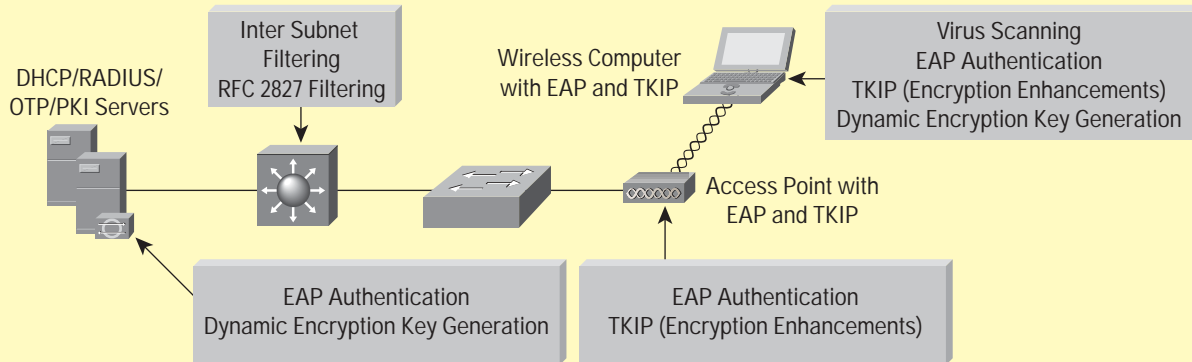
While 802.1X authentication types provide strong authentication for wireless LANs, standard 802.11 WEP encryption is still vulnerable to network attacks. The Cisco Wireless Security Suite supports TKIP for both static and dynamic encryption keys. Like WEP, TKIP uses an encryption method developed by engineer Ron Rivest, known as Ron’s Code 4 (RC4) encryption. However, TKIP adds measures such as per-packet key hashing, MIC, and broadcast key rotation to address known vulnerabilities of WEP.

With the Cisco Wireless Security Suite, both Cisco TKIP and WPA TKIP algorithms are available on Cisco Aironet access points and Cisco and Cisco Compatible WLAN client devices. Although Cisco TKIP and WPA TKIP do not interoperate, Cisco Aironet Series access points can run both Cisco TKIP and WPA TKIP simultaneously when using multiple VLANs. System administrators will need to choose one set of TKIP algorithms to activate on the enterprise’s client devices because clients cannot support both sets of TKIP algorithms simultaneously.

For deployments using Cisco client devices exclusively, Cisco TKIP is recommended for both access points and clients. In mixed-client environments, both Cisco TKIP and WPA TKIP algorithms are recommended on the access points to allow existing Cisco and Cisco Compatible client devices to use Cisco TKIP, with WPA TKIP recommended for all other client devices.

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 such as AirSnort, an intruder can exploit this flaw by gathering packets encrypted with the same key and using the weak IVs to calculate the base key.

Cisco TKIP and WPA TKIP include key hashing, or per-packet keying, to mitigate weak IV attacks. When key-hashing support is implemented on both the access point 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 helping to ensure 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.

Message Integrity Check Protection from Active Network Attacks

The use of a MIC thwarts an active network attack designed to determine the encryption key used to encrypt intercepted packets. This active attack is a combination of a bit-flipping attack and a replay attack. When MIC support is implemented on both the access point 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.

Broadcast-Key Rotation

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

SECURITY ENHANCEMENTS

ATTACKS	SECURITY ENHANCEMENTS		
	Authentication: Open Encryption: Static WEP	Authentication: Cisco LEAP, EAP-TLS or PEAP Encryption: Dynamic WEP	Authentication: Cisco LEAP, EAP-TLS or PEAP Encryption: Cisco TKIP, WPA TKIP, AES
Man-in-the-Middle	■	■	●
Authentication Forging	■	●	●
Weak IV Attacks (AirSnort)	■	■	●
Packet Forgery (Replay Attack)	■	■	●
Brute-Force Attacks	■*	●**	●**
Dictionary Attacks	■	●**	●**

■ Vulnerable
● Protected

* 40-bit WEP vulnerable.

** Strong passwords required with Cisco LEAP. Read more in Section 5.2 of the 802.11 Wireless LAN Security White Paper.

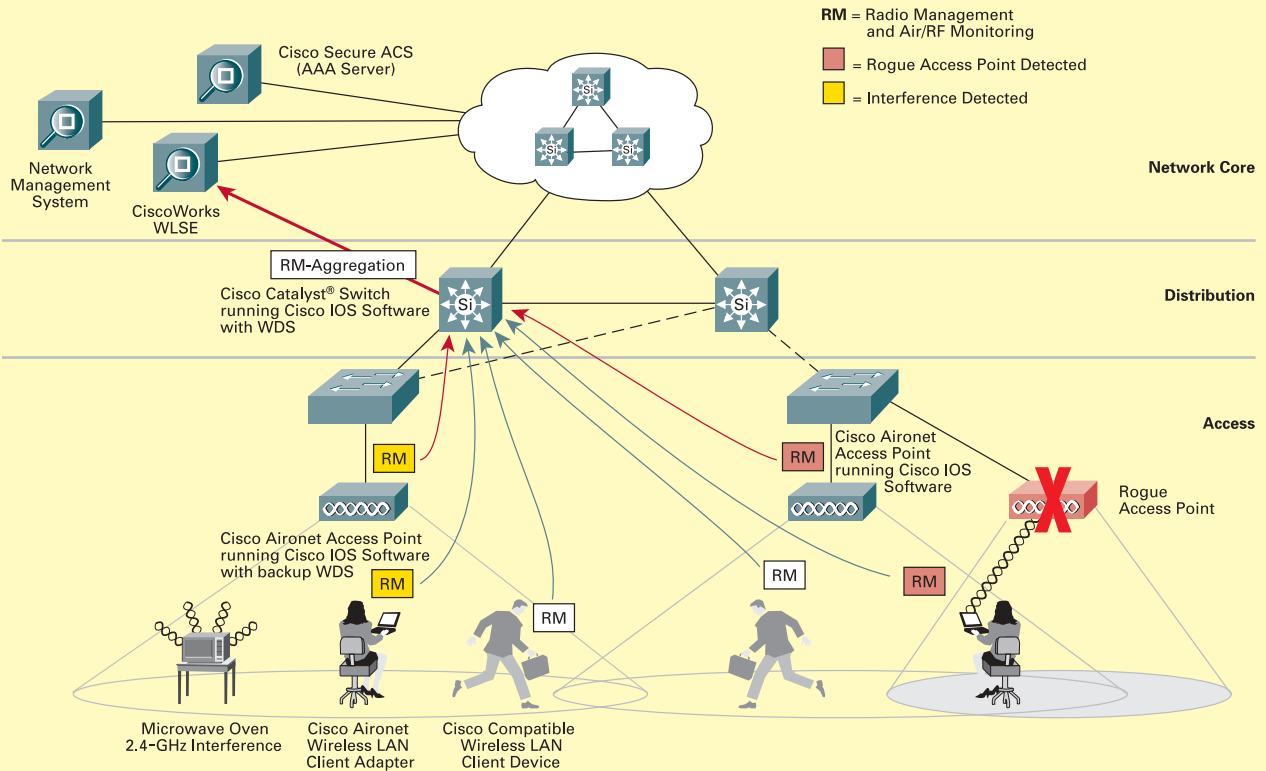
IEEE 802.11i, WPA2, and Advanced Encryption Standard

In 2004, the Cisco Wireless Security Suite will also support IEEE 802.11i and WPA2. IEEE 802.11i is the proposed IEEE standard for WLAN security, and WPA2 is the successor to WPA. Both 802.11i and WPA2 include AES as an alternative to TKIP.

Cisco Structured Wireless-Aware Network

Network managers need WLANs that provide the same level of security, scalability, reliability, ease of deployment, and management that they have come to expect from their wired LANs. The Cisco Structured Wireless-Aware Network (SWAN) is a secure, integrated wireless LAN (WLAN) solution of Cisco “wireless-aware” infrastructure products that minimizes WLAN total cost of ownership through optimized deployment and management of market-proven, high-performance, multi-function Cisco Aironet Series access points. Cisco SWAN extends to the wireless LAN the same level of security, scalability, reliability, ease of deployment, and management that customers have come to expect in their wired LANs.

Cisco SWAN includes four core components. Functionality can be extended through Cisco and Cisco Compatible client devices and, in the future, through wireless-aware Cisco wired infrastructure products for integrated wired and wireless LAN capabilities.



1. Clients and access points send their Radio Management (RM) data to the Cisco access point, switch or router running wireless-aware Cisco IOS Software with Wireless Domain Services (WDS).
2. Cisco access point, switch or router running wireless-aware Cisco IOS Software with WDS uses RM-Aggregation to condense and digest the RM data into a set of small messages that it sends to the CiscoWorks WLSE.

Core Components

- Cisco Aironet Series access points running Cisco IOS® Software
- CiscoWorks Wireless LAN Solution Engine (WLSE)
- IEEE 802.1X authentication server, such as the Cisco Secure Access Control Server (ACS)
- Wi-Fi Certified WLAN client adapters

Optional Components


For a full range of enterprise-class security options, including all 802.1X authentication types and extended air/radio frequency (RF) radio management capabilities, add:

- Cisco Aironet wireless LAN client adapters
- Cisco Compatible wireless LAN client devices

Future Components

For integrated wired and wireless LAN networks, add:

- Cisco switches and routers running wireless-aware Cisco IOS Software (available starting in calendar year 2004)



Cisco SWAN minimizes the total cost of ownership and maximizes wireless network uptime and security by optimizing the following:

Deployment

- Assisted site surveys
- “Live” air/RF scanning and monitoring
- Interference detection
- Auto-configuration of new access points

Management

- Simplified, automated air/RF operation of hundreds to thousands of central or remotely located access points from a single management console
- Enhanced troubleshooting, diagnostic tools, and client and usage reports
- High availability with self-healing wireless LANs (future)
- Mass configuration and firmware updates
- XML API for data export

Security

- Rogue access point detection and location
- WAN link remote site survivability
- Security policy monitoring and alerts
- Centralized security settings for parameters such as 802.1X EAP and WPA
- Full access control and privacy with fast secure layer 2 roaming and (future) fast secure layer 3 roaming

Flexibility

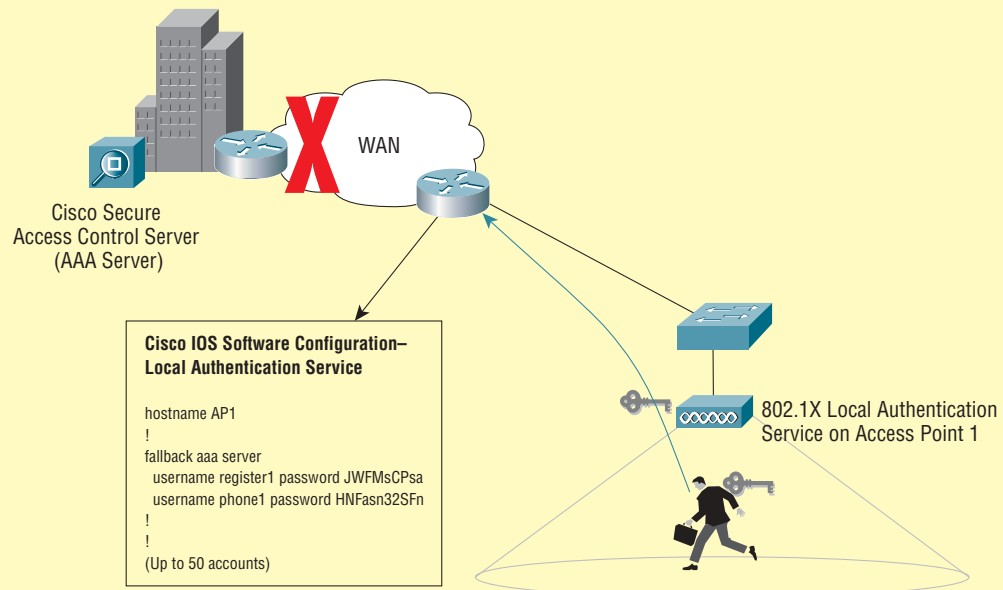
- Integrated wired and wireless LAN services using the Cisco infrastructure and Cisco IOS Software
- Cisco switch and router enhancements (future)

Support

- Cisco warranties, support services, and partnerships like the Cisco Compatible Extensions program

Detecting Rogue Access Points

Having the ability to detect rogue access points is critical to maintaining a secure WLAN. Rogue (or unauthorized) access points installed by employees or intruders create security breaches that put the entire network at risk. With Cisco SWAN, the process of detecting rogue access points is automated. IT managers can easily and automatically detect, locate, and disable rogue access points and the switch ports to which they are connected because both access points and client devices actively participate in continuous scanning and monitoring of the RF environment.



WAN Link Remote Site Survivability

Remote site survivability is enabled via the access point's IEEE 802.1X local authentication service. With IEEE 802.1X local authentication service, Cisco Aironet access points are configured to act as a local authentication server to authenticate wireless clients when the AAA server is not available. This provides secure authentication services for remote or branch office WLANs without a RADIUS server and backup authentication services, for access to local resources such as file servers or printers, during a wide area network (WAN) link or server failure.

Summary

With the Cisco Wireless Security Suite's 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 compromising network security.

The Cisco Aironet product line easily integrates with an existing network. Its mobility and flexibility make it the best solution for secure wireless networking and it's easy to install. Deployment assistance is available through Cisco Total Implementation Solutions (TIS), and technical operational support is offered through Cisco SMARTnet® support.

See how easy it can be to launch a secure Cisco Aironet wireless network in your facilities. Read more about Cisco SWAN at www.cisco.com/go/swan. Read more about WLAN security at the Cisco Wireless LAN Security Web site at www.cisco.com/go/aironet/security, or call your Cisco account manager or sales channel partner for more information.

**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 International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

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 6317 7777
Fax: +65 6317 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.com 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

 Copyright © 2003 Cisco Systems, Inc. All rights reserved. CCIP, CCSP, the Cisco Arrow logo, the Cisco Powered Network mark, Cisco Unity, Follow Me Browsing, FormShare, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, Fast Step, GigaStack, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, MGX, MICA, the Networkers logo, Networking Academy, Network Registrar, Packet, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, ScriptShare, SlideCast, SMARTnet, StrataView Plus, Stratm, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0304R)