

Give Your Network Users Freedom and Mobility Without Giving Up Network Security



CISCO WIRELESS LAN PRODUCTS—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 via the [Cisco Unified Wireless Network](#), Cisco offers an enterprise-ready, standards-based, WLAN security solution that supports the following features for [Cisco wireless products](#), [Cisco Aironet® products](#), and [Cisco Compatible WLAN client devices](#).

- Support for the IEEE 802.11i standard
- Support for the Wi-Fi Alliance security certifications Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access 2 (WPA2)
- Strong, mutual authentication and dynamic encryption key management via support for IEEE 802.1X
- Data encryption using Advanced Encryption Standard (AES) or Temporal Key Integrity Protocol (TKIP)
- Support for the broadest range of 802.1X authentication types, client devices, and client operating systems on the market
- Mitigation of active and passive network attacks
- Integration with the Cisco Self-Defending Network and [Network Admission Control](#) (NAC)
- Intrusion Prevention System (IPS) capabilities and advanced location services with real-time network visibility
- Indoor/outdoor Wi-Fi security convergence with Cisco's wireless mesh solution
- Management Frame Protection (MFP) to provides strong cryptographic authentication of WLAN management frames for the detection and prevention of 802.11 management frame attacks

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 Wired Equivalent Privacy (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.

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), IPS, 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 Unified Wireless Network, network managers can decrease risks to their network and increase WLAN security.

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.

Figure 1. Multiple plenum-rated Cisco Aironet autonomous or lightweight access points can be placed throughout a building or campus to maintain fully secure, uninterrupted access to all network resources. Cisco Aironet access points provide users equipped with Cisco Aironet, Cisco Compatible or Wi-Fi Certified WLAN client adapters with the ability to move freely about covered areas of the campus.



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 or WPA 2 Pre-Shared Key

Another form of basic security now available is WPA or WPA2 Pre-Shared Key (PSK). The PSK verifies users via a password, or identifying code, (also called a passphrase) 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 PSK also provides keying material that TKIP or AES use to generate an encryption key for each packet of transmitted data. While more secure than static WEP, 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/WPA2 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

Enhanced security is recommended for those customers requiring enterprise-class security and protection. The Cisco Unified Wireless Network delivers an enhanced wireless security solution that provides full support for WPA and WPA2 with its building blocks of 802.1X mutual authentication and TKIP or AES encryption. The Cisco Unified Wireless Network includes the following:

- 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
- AES for government-grade, highly secure data encryption
- Integration with the Cisco Self-Defending Network and NAC
- Intrusion Prevention System (IPS) capabilities and advanced location services with real-time network visibility
- Management Frame Protection (MFP) for strong cryptographic authentication of WLAN management frames

Detailed information about the Cisco Unified Wireless Network's enterprise-class wireless security is provided later in this document.

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.

For enterprise deployments, an enhanced security solution, such as the Cisco Unified Wireless Network, meets and exceeds WLAN security requirements, so using a VPN for an enterprise WLAN is not necessary. Using VPN in an internal WLAN deployment may affect WLAN performance, limit roaming and make the login process more complex for users. Therefore, the additional overhead, limitations, and expense of a VPN overlay for an internal WLAN are not necessary.

PEACE OF MIND WITH THE CISCO UNIFIED WIRELESS 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. Security policy monitoring must be performed on a regular basis. Network security solutions must be easily deployable to several, hundreds or thousands of access points. Unauthorized access points installed by employees or malicious intruders must be detected.

The Cisco Unified Wireless Network supports an enterprise-ready, standards-based, wireless security solution that gives network administrators' confidence that their data will remain private and secure when they use Cisco wireless products, [Cisco Aironet Series](#) products, [Cisco Compatible Extensions](#) products, or Wi-Fi Certified WLAN client devices. This enterprise-class wireless security solution supports robust wireless LAN security services that closely parallel the security available in a wired LAN. It fulfills the need for consistent, reliable, and secure mobile networking by delivering industry-leading WLAN security services. It mitigates sophisticated passive and active WLAN attacks, interoperates with a range of client devices and provides reliable, scalable, centralized security management. The Cisco Unified Wireless Network allows network administrators to deploy large-scale enterprise WLANs with scalable problem-free security administration that does not increase the burden on the IT staff.

The Cisco Unified Wireless Network delivers many innovative Cisco enhancements and supports [Wi-Fi Protected Access](#) (WPA) and [Wi-Fi Protected Access 2](#) (WPA2) providing access control via per-user, per-session mutual authentication and data privacy via strong dynamic encryption. Quality of service (QoS) and mobility are integrated into this solution to enable a rich set of enterprise applications.

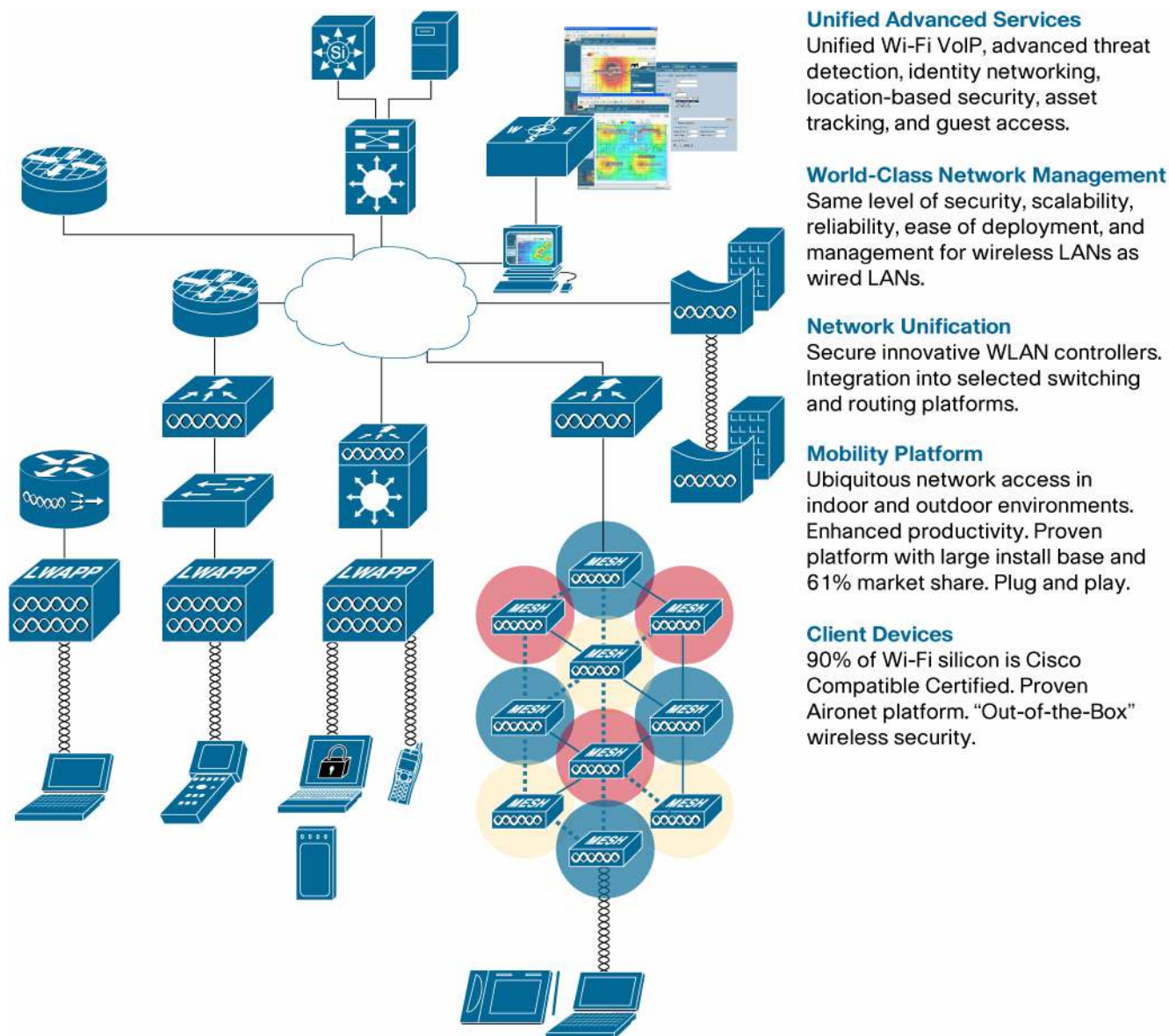
The Cisco Unified Wireless Network provides:

- **Secure Connectivity for WLANs**—Strong dynamic encryption keys that automatically change on a configurable basis to protect the privacy of transmitted data.
 - WPA—TKIP encryption enhancements such as MIC, per-packet keys via initialization vector hashing, and broadcast key rotation
 - WPA2—AES the “gold standard” for data encryption
- **Trust and Identity for WLANs**—Robust WLAN access control that helps to ensure that legitimate clients associate only with trusted access points rather than rogue or unauthorized access points. This is provided via per-user, per-session, mutual authentication using IEEE 802.1X, a variety of Extensible Authentication Protocol (EAP) types and a Remote Authentication Dial-In User Service (RADIUS) or Authentication, Authorization, and Accounting (AAA) server.
 - Support for the broadest range of 802.1X authentication types, client devices, and client operating systems on the market
 - Support for RADIUS accounting records for all authentication attempts

- **Threat Defense for WLANs**—Detection of unauthorized access, network attacks and rogue access points via a robust IPS, WLAN NAC, and advanced location services. Cisco's enterprise-class IPS allows IT managers to continually scan the RF environment, detect rogue access points and unauthorized events, simultaneously track thousands of devices, and mitigate network attacks. NAC has been designed specifically to help ensure that all wired and wireless endpoint devices (such as PCs, laptops, servers, and PDAs) accessing network resources are adequately protected from security threats. NAC allows organizations to analyze and control all devices coming into the network.

The Cisco Unified Wireless Network is the industry's only unified wired and wireless solution to cost-effectively address the WLAN security, deployment, management, and control issues facing enterprises. This powerful solution combines the best elements of wireless and wired networking to deliver scalable, manageable, and secure WLANs with a low total cost of ownership. It includes innovative RF capabilities that enable real-time access to core business applications and provides proven enterprise-class secure connectivity. The Cisco Unified Wireless Network is an integrated end-to-end solution that addresses all layers of the WLAN, from client devices and access points, to the network infrastructure, to network management, to the delivery of advanced wireless services integration and award-winning, worldwide, 24-hour product support. (Figure 2)

Figure 2. Cisco Unified Wireless Network



WPA and WPA2 Support

The Cisco Unified Wireless Network includes support for the Wi-Fi Alliance certifications WPA and WPA2. WPA was introduced by the Wi-Fi Alliance in 2003. WPA2 was introduced by the Wi-Fi Alliance in 2004. All products Wi-Fi Certified for WPA2 are required to be interoperable with products that are Wi-Fi Certified for WPA.

WPA and WPA2 offer a high level of assurance for end users and network administrators that their data will remain private and that access to their networks will be restricted to authorized users. Both have personal and enterprise modes of operation that meet the distinct needs of the two market segments. The Enterprise Mode of each uses IEEE 802.1X and EAP for authentication. The Personal Mode of each uses PSK for authentication. Cisco does not recommend Personal Mode for business or government deployments because it uses a PSK for user authentication. PSK is not secure for enterprise environments.

WPA addresses all known WEP vulnerabilities in the original IEEE 802.11 security implementation bringing an immediate security solution to WLANs in both enterprise and small office/home office (SOHO) environments. WPA uses TKIP for encryption.

WPA2 is the next generation of Wi-Fi security. It is the Wi-Fi Alliance's interoperable implementation of the ratified IEEE 802.11i standard. It implements the National Institute of Standards and Technology (NIST) recommended AES encryption algorithm using Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP). WPA2 facilitates government FIPS 140-2 compliance. (Table 1)

Table 1. Comparison of WPA and WPA2 Mode Types

	WPA	WPA2
Enterprise Mode (Business, Government, Education)	<ul style="list-style-type: none">• Authentication: IEEE 802.1X/EAP• Encryption: TKIP/MIC	<ul style="list-style-type: none">• Authentication: IEEE 802.1X/EAP• Encryption: AES-CCMP
Personal Mode (SOHO, Home/Personal)	<ul style="list-style-type: none">• Authentication: PSK• Encryption: TKIP/MIC	<ul style="list-style-type: none">• Authentication: PSK• Encryption: AES-CCMP

IEEE 802.1X Authentication and the Extensible Authentication Protocol

The IEEE has adopted 802.1X as a standard for authentication on wired and wireless networks. 802.1X is supported by both WPA-Enterprise Mode and WPA2-Enterprise Mode. 802.1X 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. While 802.1X authentication types provide strong authentication for wireless LANs, TKIP or AES are needed for encryption in addition to 802.1X since standard 802.11 WEP encryption, is vulnerable to network attacks.

Several 802.1X authentication types exist, each providing a different approach to authentication while relying on the same framework and 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-Flexible Authentication via Secure Tunneling](#) (EAP-FAST), EAP-Transport Layer Security (EAP-TLS), [Protected Extensible Authentication Protocol](#) (PEAP), EAP-Tunneled TLS (EAP-TTLS), and EAP-Subscriber Identity Module (EAP-SIM).

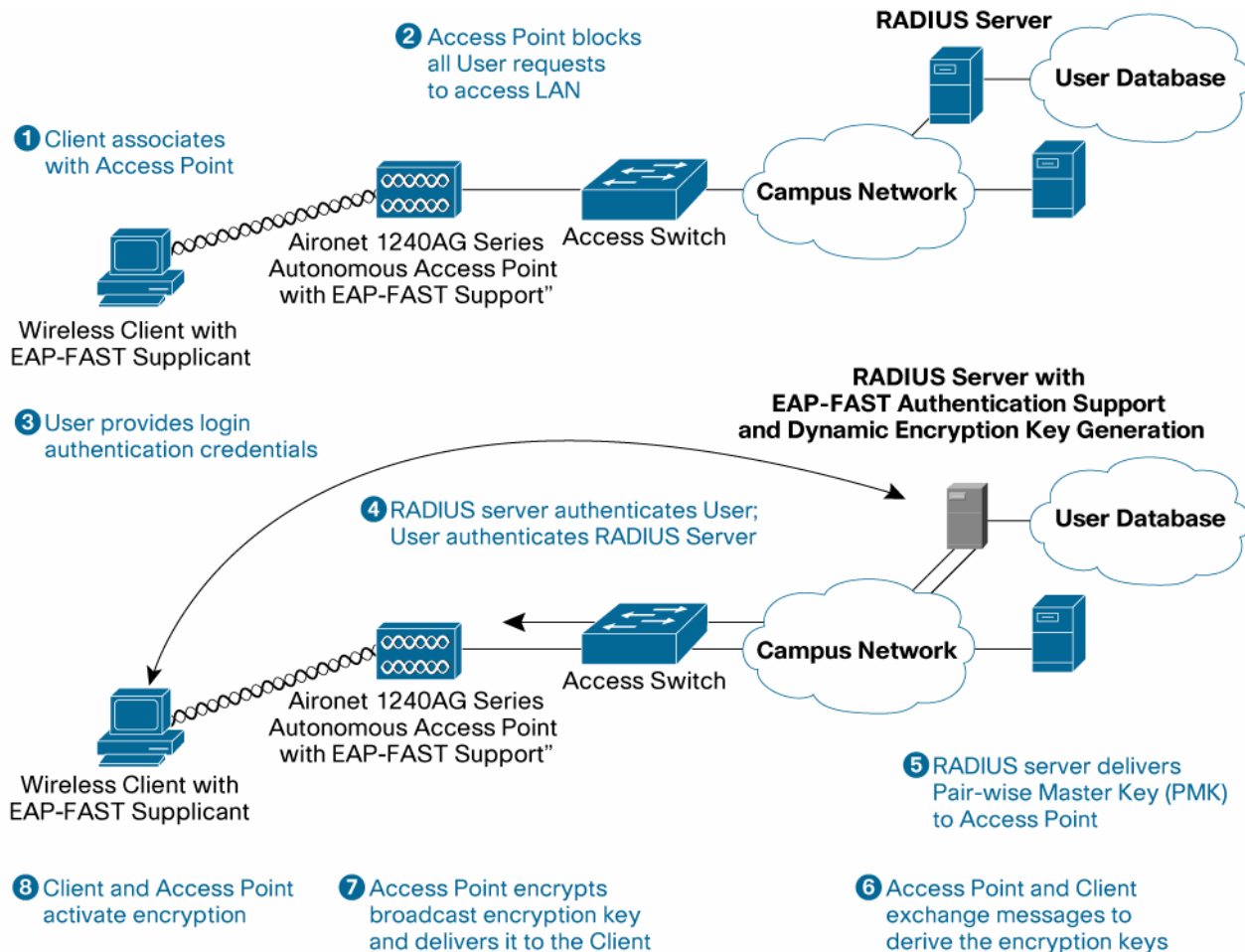
Cisco recommends that customers evaluate their networks and security environments to select the best EAP authentication type for their 802.1X deployment. Areas to evaluate when selecting an EAP type include the type of security mechanism used for security credentials, the user authentication database, the client operating systems in use, the available client supplicants, the type of user login needed, and RADIUS or 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 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. (Figure 3)

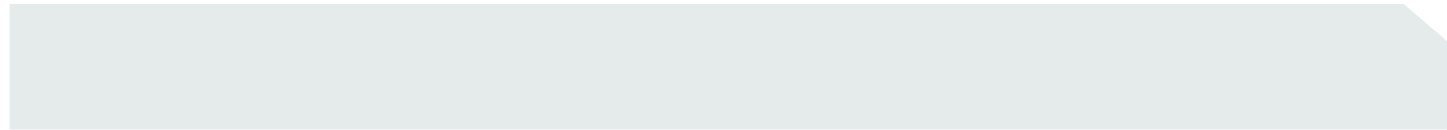
Figure 3. The Cisco Unified Wireless Network for Enterprise-Class Security



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 autonomous access point or wireless LAN controller, 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 name/ID and SSID parameters are passed to the autonomous access point or wireless LAN controller. When the autonomous access point or wireless LAN controller receives the VLAN name/ID assignment for a specific user, it places that user on the specified VLAN name/ID. If the allowed SSID list is also passed to the access point or controller, the access point or controller will help ensure that the user is providing a valid SSID to access the WLAN. If the user provides an SSID not specified in the allowed SSID list, the access point or wireless LAN controller disassociates the user from the WLAN network.

The Cisco Unified Wireless Network supports Simple Network Management Protocol Version 3 (SNMPv3), Secure Shell (SSH) Protocol (secure Web), and SSL (secure Telnet) interfaces to the Cisco Wireless Control System (WCS). Furthermore, the Cisco WCS is configurable such that management is not possible over the air, and it supports a separate management VLAN so only stations on a specific VLAN can modify the WLAN network settings.

Management Frame Protection (MFP) provides strong cryptographic authentication of WLAN management frames for the detection and prevention of 802.11 management frame attacks. This provides for more accurate detection capabilities against 802.11 exploit tools. Not only is this effective against known attacks, but also any future attacks that rely on the unprotected nature of the WLAN management frames.

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 2104 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.

WPA Encryption—Temporal Key Integrity Protocol

The Cisco Unified Wireless Network supports TKIP, a WPA component and an IEEE 802.11i standard. TKIP is an enhancement to WEP security. Like WEP, TKIP uses an encryption method developed by engineer Ron Rivest, known as Ron’s Code 4 (RC4) encryption. However, TKIP enhances WEP by adding measures such as per-packet key hashing, MIC, and broadcast key rotation to address known vulnerabilities of WEP.

TKIP uses the RC4 stream cipher with 128-bit keys for encryption and 64-bit keys for authentication. By encrypting data with a key that can be used only by the intended recipient of the data, TKIP helps to ensure that only the intended audience understands the transmitted data. TKIP encryption can generate up to 280 trillion possible keys for a given data packet.

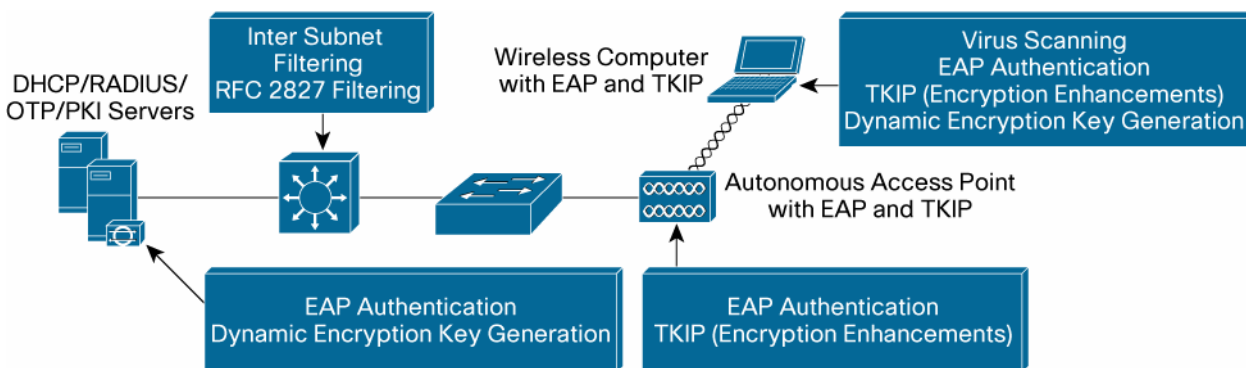
With the Cisco Unified Wireless Network, both Cisco TKIP and WPA TKIP algorithms are available on Cisco Aironet autonomous access points and Cisco Aironet and Cisco Compatible WLAN client devices. Although Cisco TKIP and WPA TKIP do not interoperate, Cisco Aironet Series autonomous access points can 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. Cisco recommends that WPA TKIP be used for client devices and access points wherever possible. Cisco wireless LAN controllers and Cisco Aironet lightweight access points support only WPA TKIP.

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 TKIP 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.

TKIP includes 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. (Figure 4)

Figure 4. Attack Mitigation Roles for WPA—802.1X EAP/TKIP WLAN Design



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

TKIP 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.

WPA2 Encryption—Advanced Encryption Standard

The Cisco Unified Wireless Network supports WPA2 which uses the AES encryption scheme for confidentiality and integrity. AES is an alternative encryption scheme to the RC4 encryption used in TKIP and WEP. AES has no known attacks and offers stronger encryption than TKIP and WEP. AES is an extremely secure cryptographic algorithm with current analysis indicating that it takes 2^{120} operations to break an AES key—a feat not yet accomplished.

AES is a block cipher which is a type of symmetric key cipher that uses the same key for both encryption and decryption and uses groups of bits of a fixed length—called blocks. Unlike WEP which uses a key stream acting across a plaintext data input stream for encryption, AES encrypts bits in blocks of plaintext that are independently calculated. The AES standard specifies an AES block size of 128 bits with three possible key lengths 128, 192 and 256 bits. A 128 bit key length is used for WPA2/802.11i. One round of WPA2/802.11i AES encryption is made up of four stages. With WPA2/802.11i, each round is iterated 10 times.

To provide both data confidentiality and authenticity, a new mode of construction called Counter-Mode/CBC-Mac (CCM) is used with AES. CCM employs AES in Counter mode (CTR) to achieve data confidentiality and AES using Cipher Block Chaining Message Authentication Code (CBC-MAC) to provide data integrity. This type of construction, one that uses one key for two modes (CTR and CBC-MAC) is a “new” construction that has been accepted by NIST (Special Publication 800-38C) and the standard community (IETF RFC-3610).

A 48-bit IV is used for CCM. Like TKIP, AES does not use the IV in the same manner as WEP encryption methods. With CCM, the IV is used as an input to the encryption and decryption processes to mitigate replay attacks. Also, since the IV space is expanded to 48 bits, the time required to incur an IV collision is increased exponentially—providing greater data protection.

It is recommended that AES encryption (and decryption) be performed in hardware because of the computationally intensive nature of AES. Cisco wireless products perform AES encryption in hardware. Performing AES encryption in software for multiple clients simultaneously requires horsepower, such as that offered by a 2.5-GHz Pentium processor laptop for example. If an access point performed AES encryption/decryption in software while serving numerous associated clients, the access point likely would incur performance degradation, especially if that access point lacked a powerful processor and a large amount of RAM and ROM.

WPA and WPA2 Deployment

Cisco recommends that customers use WPA2 for client devices that support WPA2. Although WPA is still considered secure and TKIP has not been broken, Cisco recommends that customers’ transition to WPA2 as soon as they can. Because WPA2 requires configuration changes to both access points and client devices, the introduction of WPA2 should be planned and large sets of client devices and access points should be transitioned at the same time to minimize network disruption. One opportunity for a transition to WPA2 is when a wireless network is introduced, upgraded, or expanded.

To make the transition to WPA and WPA2 easier, Cisco Aironet autonomous access points support both WPA Migration Mode and WPA2 Mixed Mode. WPA Migration Mode is an autonomous access point setting defined by Cisco that enables both WPA and non-WPA clients to associate to an access point using the same SSID. WPA Migration Mode should only be used as a temporary transition mode since it supports the authentication of WEP clients and is therefore potentially insecure. WPA2 Mixed Mode operation permits the coexistence of WPA and WPA2 clients on a common SSID. WPA2 Mixed Mode is a Wi-Fi Certified feature. WPA2 Mixed Mode is considered secure since it uses both TKIP and AES for encryption.

Specialized WLAN client devices may not be able to run AES and may not be upgradable to AES (and WPA2). Therefore, Cisco recommends that enterprise organizations continue to use and deploy WPA for these devices as applicable. All networks should run WPA as a minimum.

Read the [Wi-Fi Protected Access, WPA2 and IEEE 802.11i Q&A](#) for more information.

Protection from Network Attacks

A variety of attacks can be issued against WLANs. Both WPA and WPA2 protect the network from a variety of network attacks when 802.1X, EAP types and TKIP or AES are used. (Figure 5)

Figure 5. New Security Enhancements Mitigate Network Attacks

SECURITY ENHANCEMENTS			
ATTACKS	Authentication: Open Encryption: Static WEP	Authentication: Cisco LEAP, EAP-FAST, EAP-TLS or PEAP Encryption: Dynamic WEP	Authentication: Cisco LEAP, EAP-FAST, 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.

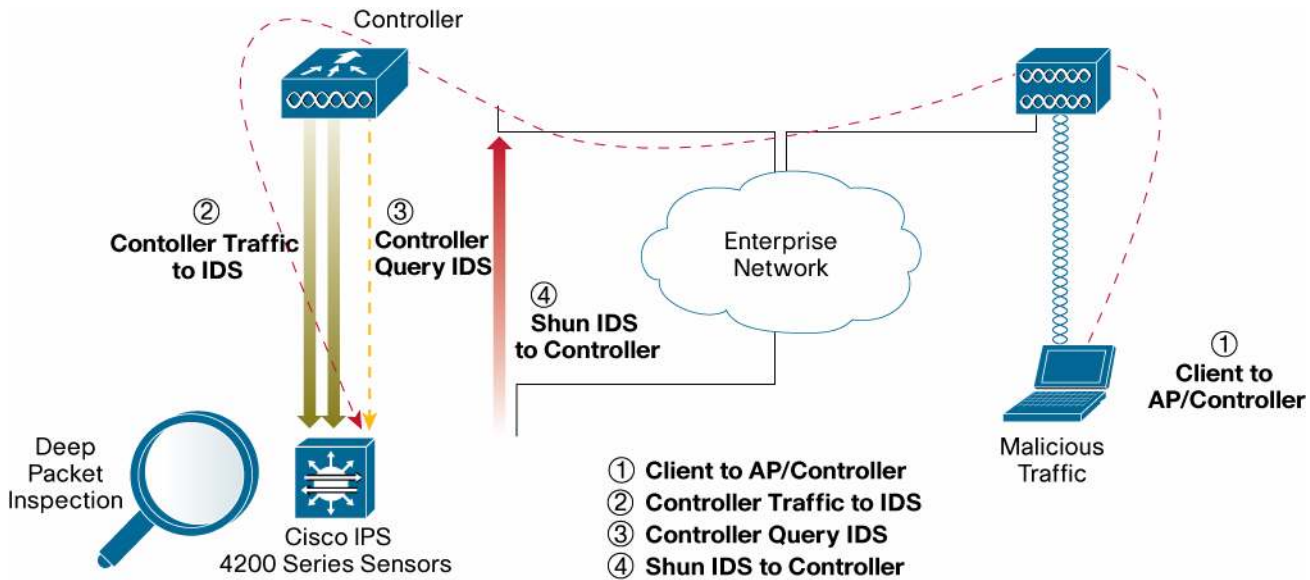
WLAN Intrusion Prevention System

In the Cisco Unified Wireless Network, access points simultaneously act as air monitors and data forwarding devices. This setup allows access points to communicate real-time information about the wireless domain, including potential security threats to Cisco Wireless LAN controllers, without interrupting service. All security threats are rapidly identified and presented to network administrators through the Cisco WCS, where accurate analysis can take place and corrective action can be taken.

If your company has a “no Wi-Fi” policy, you can deploy the Cisco Unified Wireless Network initially as a standalone wireless IPS, and later reconfigure it to add WLAN data service. This scenario allows your network managers to create a “defense shield” around your RF domains, containing unauthorized wireless activity until your organization is ready to deploy WLAN services. Cisco Systems provides the only WLAN system that offers simultaneous wireless protection and WLAN service delivery, helping to ensure complete WLAN protection with no unnecessary overlay equipment costs or extra monitoring devices.

The Cisco Unified IDS/IPS is part of the Cisco Self-Defending Network and is the industry’s first integrated wireline and wireless security solution. The Cisco Unified IDS/IPS takes a holistic approach to security—at the wireless edge, wired edge, WAN edge and through the data center. When an associated client sends malicious traffic through the Unified Wireless network, a Cisco wireline IDS device detects the attack and sends shun requests to Unified WLAN controllers which will then disassociate the client device (Figure 6).

Figure 6. Cisco Unified IDS/IPS Detects Malicious Attacks Allowing the WLAN Controller to Disassociate the Offending Client Device



NAC for WLANs

NAC is a set of technologies and solutions built on an industry initiative led by Cisco Systems®. NAC uses the network infrastructure to enforce security policy compliance on all devices seeking to access network computing resources, thereby limiting damage from emerging security threats such as viruses, worms, and spyware. Customers using NAC can allow network access only to compliant and trusted endpoint devices and can restrict the access of noncompliant devices. NAC is part of the Cisco Self-Defending Network, a strategy to dramatically improve the network's ability to automatically identify, prevent, and adapt to security threats.

Cisco offers both the [NAC Appliance](#) and the [NAC Framework](#) to meet the functional and operational needs of any organization, whether they have a simple security policy requirement or require support for a complex security implementation involving a number of security vendors, combined with a corporate desktop management solution.

Both the NAC Appliance and the NAC Framework provide security threat protection for WLANs by enforcing device security policy compliance when WLAN clients attempt to access the network. These solutions quarantine non-compliant WLAN clients and provide remediation services to help ensure compliance. Both solutions are fully interoperable with the Cisco Unified Wireless Network. Additional information about NAC for WLANs is available in the [Cisco Network Admission Control for Wireless LANs Solution Overview](#).

WAN Link Remote Site Survivability

Cisco Aironet autonomous access points support remote site survivability. This capability is enabled via the autonomous access point's IEEE 802.1X local authentication service. With IEEE 802.1X local authentication service, Cisco Aironet autonomous 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 Unified Wireless Network's security features properly configured and activated, network administrators can feel confident that their company data will remain private and secure. This solution provides network managers with the same level of security, scalability, reliability, ease of deployment, and management for wireless LANs that they have come to expect from their wired LAN. The Cisco Unified Wireless Network fully integrates with the Cisco Self-Defending Network and NAC and allows network managers to give their end users freedom and mobility without compromising network security.

The Cisco Aironet product line, supporting both autonomous and lightweight access points, 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 wireless network in your facilities.

For more information about Cisco Aironet products please visit, <http://www.cisco.com/go/aironet>

For more information about the Cisco wireless security please visit, <http://www.cisco.com/go/aironet/security>

For more information about Cisco Unified Wireless Network please visit, <http://www.cisco.com/go/unifiedwireless>

For more information about NAC, please visit, http://www.cisco.com/en/US/netsol/ns466/networking_solutions_package.html

For more information about WPA, WPA2 and 802.11i, please visit,
http://www.cisco.com/en/US/prod/collateral/wireless/ps5678/ps430/prod_qas0900aecd801e3e59.shtml

For more information about the Wi-Fi Alliance WPA certification please visit, <http://www.wi-fi.com>

For more information about the Wi-Fi Alliance WPA2 certification please visit, <http://www.wi-fi.com>



Americas 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: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

©2007 Cisco Systems, Inc. All rights reserved. CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, Packet, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website 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. (0705R)