



White Paper

Addressing Wireless Threats with Integrated Wireless IDS and IPS in the Cisco Unified Wireless Network

This paper describes rogue access points and other wireless threats and how the Cisco Unified Wireless Network detects and prevents them.

SUMMARY

Wireless LAN security has improved dramatically since the introduction of IEEE 802.11 in 1997. When the most recent security standard, IEEE 802.11i, is employed, wireless networks are as secure—or more secure—as many wired network implementations. However, because of the ability of wireless LANs to penetrate beyond the physical boundaries of an enterprise, wireless threats exist from unauthorized infrastructure and clients. The good news for IT managers is that these threats can be detected and prevented using the Cisco Unified Wireless Network while it simultaneously provides service to wireless clients. Enterprises that do not yet wish to deploy a production wireless LAN system can deploy the Cisco® Unified Wireless Network in a monitor-only mode to ensure that wireless threats do not compromise the integrity of their wired networks and lead to the loss of confidential information, a decrease in customer confidence, or possible regulatory violations.

CHALLENGE

While IT administrators may already be aware of the proper techniques for securing the wireless LAN using 802.11i, they may be surprised to learn that this alone is not enough to protect the enterprise. Whether an enterprise has an authorized WLAN or a no Wi-Fi policy, it is important to be aware of the vulnerability that the hardwired corporate network has to wireless threats. The most common is the rogue access point. Eager employees often bring in their own access points—typically consumer-grade and very low cost—to speed wireless connectivity in their department, unaware of the dangers. These rogue access points are behind the firewall and are not detectable by intrusion detection or intrusion prevention systems (IDS/IPS) used by traditional wired networks. Anyone within range of the signal can attach and access the corporate network.

Complicating the security challenge is the new reality of mobile workers requiring access to the corporate network off premises as well as on. The home, hotels, airports, and other wireless hotspots are all regularly used by corporate employees to conduct business. Because laptops are at risk for contracting viruses, spyware, and malware, these unmanaged sites can act as a conduit for threats to the corporate network. Wireless clients can exacerbate the problem by connecting to wireless access points or other wireless clients without the user's knowledge.

SOLUTION

Cisco's Self-Defending Network strategy protects against the new threats to corporate security posed by wireless technologies. Combined with Cisco's Integrated Security Solutions, the Cisco Unified Wireless Network provides a comprehensive solution for protecting the wired network from wireless threats as well as ensuring secure, private communications over an authorized wireless LAN. Every device in the network—from clients to access points to wireless controllers and the management system—plays a part in securing the wireless network environment through a distributed defense. This paper explains the different categories of wireless threats and how the Cisco Unified Wireless Network incorporates automatic wireless intrusion detection and prevention to protect the enterprise. For an overview of the five key steps to securing your wireless LAN, please see "[Five Steps to Securing Your Wireless LAN and Preventing Wireless Threats.](#)"

ENABLING ACCURATE THREAT DETECTION AND PREVENTION

The first step in enabling accurate wireless threat detection and prevention is to ensure that authorized wireless infrastructure and users are properly identified to the network. Without this step, any IDS/IPS will be of little value, because administrators will spend much of their time resolving false positives. The IEEE standards provide for accurate identification of authorized clients and infrastructure through 802.11i.

The IEEE 802.11i security standard uses IEEE 802.1X for mutual authentication between the network and the client. This means that clients that try to access network resources must be authenticated by the network. In a similar vein, the client verifies the authenticity of the network infrastructure it is attaching to before beginning data transmission. With 802.1X, the credentials used for authentication, such as login passwords, are never transmitted without encryption over the wireless medium. In addition, 802.1X provides dynamic per-user, per-session encryption keys, removing the administrative burden and security issues associated with static encryption keys.

While 802.1X authentication types provide strong authentication for wireless LANs, strong encryption is also needed. The original 802.11 standard included Wired Equivalent Privacy (WEP) encryption, which is vulnerable to network attacks and should be avoided today. In response to the weakness in 802.11 and in WEP and the delay in ratifying the 802.11i security standard, the Wi-Fi Alliance defined an industry standard known as Wi-Fi Protected Access (WPA). WPA uses 802.1X authentication and Temporary Key Integrity Protocol (TKIP) encryption.

In 2004, the IEEE ratified the 802.11i WLAN security standard, which includes 802.1x authentication and Advanced Encryption Standard (AES) encryption. The Wi-Fi Alliance interoperable certification of 802.11i is called WPA2. The TKIP encryption algorithm used in WPA is strong, but is not as strong as AES, and should be only used as an interim security policy until clients can be upgraded to be both WPA2 and AES capable. Whenever possible, Cisco strongly recommends implementation of WPA2 and AES to create the strongest security environment possible.

AN OVERVIEW OF COMMON WIRELESS THREATS

Once the authorized users and infrastructure are identified, the Cisco Unified Wireless Network is able to protect the enterprise against common wireless threats. Cisco Unified Wireless Network Lightweight Access Points can simultaneously serve wireless client traffic and monitor the air space, or can be used as dedicated air monitors. A more detailed discussion of the Cisco Unified Wireless Network advanced security services follows these sections on common wireless threats.

Rogue Access Points and Clients

The most common wireless threat is the rogue access point. A rogue access point is typically brought in by an employee who wants unfettered wireless access. Typically low-cost and consumer-grade, these access points often do not broadcast their presence over the wire and can only be detected over-the-air. Because they are installed by employees in their default mode, authentication and encryption are not enabled. As wireless LAN signals can traverse building walls, the danger of an open access point connected to the corporate network going undetected cannot be over emphasized. Any client that connects to a rogue access point must be considered a rogue client because it is bypassing the authorized security procedures put in place by the IT department.

Ad Hoc Networks

An ad hoc network is one that is formed directly between two client devices. Ad hoc networks pose a threat to the enterprise because the security checks imposed by the infrastructure are bypassed. One of the dangers is an employee who brings in a wireless-enabled laptop, plugs it into a wired port at work, and leaves the wireless interface enabled. In this scenario, a hacker in a neighboring area could connect directly to the client, creating a security threat. The hacker at this point could look for information on the employee's client device, and potentially gain access to the corporate network through the simultaneous wireless and wired interfaces. This situation may place the enterprise in violation of regulatory policies for its industry.

Client Misassociation

One of the benefits of wireless clients is that they quickly and easily attach to other open networks. However, this same benefit can be a potential danger to the enterprise. One such scenario occurs frequently with devices running Windows XP. In this case, the wireless configuration software will automatically connect to Service Set Identifiers (SSIDs) that have been utilized previously. If the employee has connected to a hotspot or an access point at home, and the laptop sees the same SSID while in the enterprise, it may connect automatically to an unknown access point, without the employee's knowledge. If this happens while the employee is connected to the network through a wired port, the potential exists for unknown personnel to use the wireless interface as a bridge to the enterprise's wired network. Or employees may use the neighboring wireless network in an attempt to bypass internal security controls on e-mail, instant messaging, or Internet usage policies. Both of these examples may place the enterprise in violation of regulatory policies for its industry.

Denial-of-Service Attacks and Penetration Attempts

Denial-of-service attacks are a very different type of threat to the enterprise. Instead of information or networks being exposed to unauthorized personnel, the hacker is trying to create a service disruption. Another key difference is that whereas rogue access points, client misassociation, and ad hoc networks may be unintentionally enabled by the employee, a denial-of-service (DoS) attack requires specific technical knowledge and planning and therefore is almost always a malicious act. In a DoS attack, the attacker typically spoofs management frames from the access point that a client is connected to, and de-authenticates, or disassociates WLAN clients connected to that access point. These attacks are possible because, unlike Ethernet, WLAN requires management frames for media access and collision avoidance. Because they need to be used before client stations have completed authentication, these management frames are always unauthenticated and unencrypted, even if WPA, WPA2 or a VPN are used.

In reality, very few DoS attacks are seen in corporate networks. Because the attack is perpetrated over the air, the good news is that it is highly unlikely that an entire enterprise wireless LAN network can be disabled without the hacker's physical presence being noticed. However, as more critical mobility services, such as voice over wireless LAN, come online, it will be increasingly important to quickly identify DoS attacks and precisely locate them.

Penetration attempts are of two types: man-in-the-middle attacks and offline dictionary attacks. A man-in-the-middle attack attempts to disassociate a client from a valid access point and have it reassociate with a rogue access point that is impersonating the authorized access point. The attacker will then try to capture the client's authentication information and use this to gain access to the enterprise network through the wireless LAN.

Offline dictionary attacks capture wireless data over the air and attempt to crack the encryption key. The attacker needs only to be physically nearby to collect over-the-air data and then can crack the encryption key in a separate location. If successful, the attacker may be able to use the key to gain access to the network. However, wireless LANs that employ WPA or WPA2 security cannot be breached by this type of attack.

Reconnaissance Probes

Another type of threat occurs when someone looks for open Wi-Fi signals (termed "war driving"), often using a common tool called NetStumbler. This tool, and many others like it, takes advantage of the fact that wireless networks typically broadcast their network name or SSID. Run on a handheld device with a wireless client, NetStumbler can be used to discover wireless networks in an unobtrusive manner. It is typically a passive tool, but occasionally will broadcast such that an intrusion detection system can pick it up.

The fact that network names can be discovered has been amplified by some vendors as a source of concern in an attempt to help sell dedicated wireless intrusion detection systems. This fear is misplaced. A wireless LAN that employs 802.11i (WPA2) or WPA for security cannot be breached simply through the discovery of the network name.

UNDERSTANDING PASSIVE VERSUS ACTIVE ATTACKS

In addition to understanding the various types of threats, it is also important to understand the type of attack: that is, whether the attack is passive or active, and if active, whether it is inline or offline.

In a passive attack, the perpetrator does not interact with the network, but observes data and then attempts to break into the network solely by analyzing the captured data. Examples of passive attacks include reconnaissance probes and offline dictionary attacks. There is little that can be done to prevent these types of attacks, especially with wireless LANs, because the data is transmitted over the air. The best defense against this type of attack is using the strongest known security. For this reason, Cisco recommends implementation of WPA2 and AES to create the strongest security environment possible. IT managers should be reassured that no offline dictionary attack has been successful against a WLAN employing WPA2 and AES.

Active attacks involve a hacker interacting with the network in real time. Examples of these include rogue access points, man-in-the-middle attacks, and denial-of-service attacks. Active attacks can be further classified as inline or offline. Active inline attacks are those that are launched on the channel that the WLAN is providing service on. Denial of service attacks are a good example of this, because they cannot disrupt a service unless they are on the same channel as the clients. In this case, the wireless IPS capabilities of the Cisco Unified Wireless Network provide inline protection 24 hours a day, seven days a week, since each packet is examined by the Cisco Wireless LAN Controller in real time.

Active offline attacks are those that are perpetrated on other channels, and can include threats such as rogue access points. Cisco Unified Wireless Network Lightweight Access Points can be configured to scan all wireless channels for threats. Each channel is cycled through to look for suspicious wireless activity, ensuring both inline and offline attacks are detected.

PROTECTING BRANCH OFFICES AND OTHER SITES WITHOUT WIRELESS LAN COVERAGE

Many enterprises have branch or remote offices, or portions of the main enterprise campus, that do not have wireless LAN coverage. In some respects, these areas are even more vulnerable to wireless threats because employees may bring in their own access points to gain wireless connectivity. To protect these areas, Cisco Unified Wireless Network Lightweight Access Points can be deployed as dedicated air monitors. Air monitors do not service client traffic, but are solely responsible for monitoring the air waves. All channels can be scanned and intrusion prevention techniques initiated as necessary to protect the enterprise.

An advantage of deploying the Cisco Unified Wireless Network versus an overlay wireless IDS system for this situation is that when the enterprise is ready to deploy a wireless LAN in these areas, the air monitors can be converted to service wireless clients, or additional access points can be managed by the same controller if the enterprise wishes to keep a dedicated sensor network for wireless threats. In either case, only one system needs to be deployed, learned, and maintained over time.

DETECTING AND PREVENTING WIRELESS THREATS USING THE CISCO UNIFIED WIRELESS NETWORK

The following sections explain the various strategies available to you to detect and prevent wireless security threats when you use the Cisco Unified Wireless Network.

Using Radio Resource Management to Detect Wireless Threats

The Cisco Unified Wireless Network incorporates radio resource management (RRM) to continuously monitor the surrounding air space. The radio resource management software embedded in the controller acts as a built-in RF engineer to consistently provide real-time RF management of the wireless network. RRM enables controllers to continually monitor their associated lightweight access points¹ for traffic load, interference, and other access points. RRM automatically detects and configures new controllers and lightweight access points as they are added to the network.

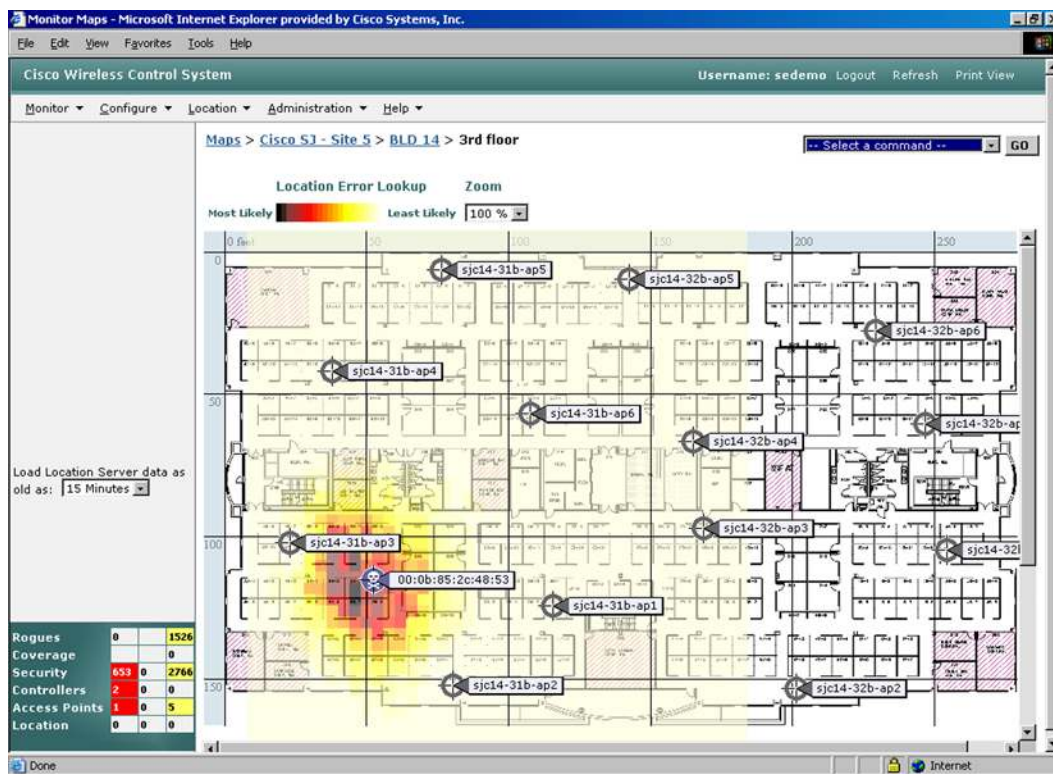
¹ For brevity, the remainder of this document will use the term access points. However, the discussion applies equally to air monitors, unless specifically noted otherwise.

Lightweight access points can be configured to detect wireless threats on all valid 802.11a/b/g channels. The access point goes “off-channel” for a period not greater than 60 ms to monitor these channels. Packets collected during this time are analyzed to detect rogue access points, rogue clients, ad-hoc clients, and all other forms of RF interference in the 2.4-GHz and 5-GHz spectrum (for example, Bluetooth signals, microwave ovens, and so on). In this way, RRM also enables the Cisco Unified Wireless Network to mitigate the effects of an RF jamming DoS attack by changing channels if excessive interference is detected in one portion of the spectrum. By default, each access point spends only 0.2 percent of its time off-channel. This activity is distributed across all access points so that adjacent access points are not scanning at the same time, which could adversely affect wireless LAN performance. In this way, administrators gain the perspective of every access point, thereby increasing network visibility.

Detecting and Preventing Rogue Access Points and Clients

Cisco Unified Wireless Network Lightweight Access Points, whether servicing clients or configured as air monitors, scan for all Wi-Fi activity. If a managed access point detects another access point over the air, and it is not managed by a Cisco Unified Wireless Network controller, it is classified as a rogue. The location of the rogue will be immediately plotted on the floor plan map (Figure 1). If investigated and found to be a neighboring wireless LAN, such as in a hotspot or adjacent business, the administrator can mark it as a “known external rogue.” Similarly, internal access points that are known, such as those in test environments, can be marked as “known internal rogues.”

Figure 1. Detected Rogue Access Points Displayed on a Map for Physical Removal



At this point, the administrator can initiate intrusion prevention. Between one and four Cisco lightweight access points contain the rogue access point by preventing clients from associating with it. This ensures that no traffic from the rogue client will reach the enterprise network until the rogue access point can be physically removed.

For sites without local IT resources, such as branch or remote offices, an automatic method to determine if the rogue access point is connected to the enterprise network is extremely beneficial. You can employ two different methods to determine if a rogue access point is connected to the enterprise network can be employed: Rogue Location Discovery Protocol (RLDP) and rogue detectors. With RLDP,

the controller instructs a managed access point to associate with the rogue access point and send a special packet to the controller. If the controller receives the packet, the rogue access point is connected to the enterprise network. This method works for rogue access points that do not have encryption enabled, which is the most likely scenario for consumer-grade access points installed by employees.

For those enterprises concerned about rogue access points that employ encryption, the Cisco Unified Wireless Network offers a method complementary to RLDP. Because a managed access point will not be able to associate with a rogue access point using encryption, a different technique must be used. In this scenario, the Cisco Unified Wireless Network monitors Address Resolution Protocol (ARP) requests sent to the network when a client associates to a rogue access point. To capture these ARP requests, rogue detectors can be deployed on the network on every wired-access VLAN. Rogue detectors are managed access points that have their radios disabled and function solely to detect and store all client ARP source MAC addresses. When the controller determines that there is a rogue access point with a client connected, it queries the rogue detectors in the network to see if they have cached an ARP from the rogue client. If the source MAC of the rogue client detected by the RF monitoring access points matches the source MAC of the rogue client detected by the rogue detector access point, the device is connected to the enterprise network.

With either of the methods just described, the rogue alarm will change from minor to critical if a rogue is determined to be connected to the enterprise network, enabling the administrator to take immediate action to prevent harmful activity.

Detecting and Preventing Ad Hoc Networks

Ad hoc networks are detected by looking at over-the-air packets and analyzing them for specific frames that indicate the connection is ad hoc, not infrastructure. Once an ad hoc network is detected, the Cisco Unified Wireless Network can prevent it by sending disassociation frames to the clients to stop the network connection.

Detecting and Preventing Client Misassociation

A unified strategy incorporating Cisco Security Agent software and the Cisco Unified Wireless Network can be deployed to not only detect, but also prevent client misassociation. The Cisco Wireless Control System (WCS) will detect and generate an alarm when a client connects to any rogue access point, enabling the administrator to take action. However, this particular threat can be eliminated by use of either Cisco Security Agent software or a third-party client firewall. Configuring the firewall to prevent simultaneous use of the wired and wireless interfaces will ensure that employees connected to the enterprise wired network will not be able to accidentally create a bridge through to their wireless enterprise. Compared with a wireless intrusion detection system alone, Cisco's unified wired and wireless security strategy provides vastly superior protection. This strategy is also much more effective than relying solely on an enterprise-based wireless IPS solution, because client misassociation can occur when a user is connected to the enterprise as a telecommuter (for example, from home or a hotel room).

Detecting and Preventing Denial-of-service Attacks and Penetration Attempts

Both DoS attacks and penetration attempts, such as the man-in-the-middle attack, rely on spoofing a management frame to de-authenticate or disassociate the client. Through the Cisco Unified Wireless Network Advanced Security Services, management frame protection (MFP) has been implemented to allow detection of a single spoofed management frame for day-zero attack protection. MFP works by hashing all management frames from the access point to the client and inserting the hash in a message integrity check (MIC) in an information element (IE) appended to the frame. By looking for a valid MIC, managed access points will detect even a single spoofed management frame and create an IDS alert for it. This is a significant improvement over other vendors' IDS implementations, which typically require a considerable number of spoofed management frames before generating an alert.

Many vendors will try to sell expensive, overlay wireless IDS solutions by citing, in a general way, the number of "attacks" that occur. However, WLAN penetration signatures are less important than detecting rogues or DoS attacks because strong wireless LAN security—that is, through WPA2 or WPA—will prevent any penetration attacks from succeeding.

In addition, many of these IDS alerts are false negatives that waste time with IT managers, causing them to hunt down unnecessary alarms. Common reasons that the IDS alert may produce false negatives include the following:

- Invalid security method—the deployment does not make use of the specific encryption and authentication method that a tool is designed to exploit. As an example, an alert that is generated for the AirJack tool is a false alarm when WEP is not used as the security method.
- Misconfigured access points. The Cisco Unified Wireless Network inherently protects against usage of nonapproved security modes by configuring all controllers and all access points from standard templates defined on the WCS. If the IT administrator has defined WPA2 or WPA as the standard security method, any lightweight access point connected to the network is guaranteed to use that template. If access points are configured separately (not centrally), misconfiguration is more likely to occur due to human error.
- Mutability of the attack signatures. Many of the attack tools are based on open source code. This makes it possible for the attacker to subtly alter the attack tool in such a way as to avoid IDS signature detection.

The Cisco Unified Wireless Network does deliver a comprehensive database of wireless attack signatures and also allows customers to define their own signatures. New releases regularly update the signature threat database. However, this is a reactive approach that merely identifies threats. Because of the problems listed with signature-based IDS attack detection, Cisco concentrates on identifying illegal WLAN behavior such as spoofed management frames, rather than on specific signatures. Once illegal WLAN behavior is identified, the Cisco Unified Wireless Network can prevent the behavior in most cases, stopping the problem rather than simply identifying it. For attacks that rely on spoofed management frames, Cisco is leading the industry towards a permanent prevention method by driving the IEEE 802.11w standards process, which will introduce encrypted management frames.

Detecting Reconnaissance Probes

As discussed earlier, reconnaissance probes such as NetStumbler that discover network names do not pose any threat to a properly secured wireless LAN. Merely knowing a network name does not provide any advantage to a hacker. The Cisco Unified Wireless Network will report reconnaissance probes such as those made by NetStumbler, but they should not be of concern. Wireless IDS vendors will seek to increase the number of the apparent attacks by including these types of tools in their signature databases, but ultimately they are no more dangerous than Windows XP automatically finding wireless network names.

DETERMINING THE LEVEL OF YOUR WIRELESS IPS INVESTMENT

You should consider several factors when determining the level of your wireless IPS investment. Cisco recommends that all enterprises have a minimum level of wireless IPS capability to protect against wireless threats such as rogue access points and denial-of-service attacks. The Cisco Unified Wireless Network delivers this capability at no additional cost through its integrated wireless IPS capabilities. Overlay wireless IPS vendors often try to heighten a negative perception of integrated wireless IPS capabilities by contending that they do not provide “continuous protection” because of the time that access points spend servicing clients. This claim is false because no sensor, whether dedicated or an access point, remains on one channel continuously; all must hop from channel to channel to scan the entire 802.11 spectrum for threats.

Cisco Unified Wireless Network access points can be deployed as sensors only, providing the same level of protection as an overlay wireless IPS solution. In fact, integrated wireless IPS solutions provide much better protection for inline attacks than overlay solutions, because integrated solutions spend most of their time on the in-use channel. In contrast, overlay solutions may need to spend equal amounts of time on each channel, and are thus more likely to not be on the channel when an attack occurs.

In contrast, an integrated solution that provides inline wireless IPS delivers unique benefits that cannot be gained from an overlay wireless IPS solution. Only an inline system that provides client services can authenticate an authorized client. Overlay systems cannot accurately determine whether a client is authorized or not through over-the-air traffic monitoring. Many overlay systems rely on over-the-air detection of a client authenticating with an authorized access points; however, this is not reliable because overlay wireless IPS sensors cannot

decrypt traffic to ascertain authenticity. An integrated solution is the only one that can provide inline detection of DoS attacks. What's more, an integrated solution minimizes upgrade costs during technology transitions, such as to 802.11n, by minimizing hardware changes to a single system instead of two. Finally, an integrated solution provides a single platform for deployment, management, and ongoing maintenance of mobility services as well as wireless IPS, reducing total cost of ownership.

SUMMARY

To properly protect the wireless LAN network and the wired enterprise network, IT administrators should first enable the strongest possible over-the-air security. Wherever possible, WPA2 should be used for strong AES encryption and mutual authentication between the network and the client. Positively authenticating the authorized clients and infrastructure is the first step in preventing wireless threats. In addition, it also renders all reconnaissance attempts from tools such as NetStumbler useless: knowing the SSID will not be of any use when strong authentication and encryption measures are in place.

Once proper identification of the authorized network components is in place, the Cisco Unified Wireless Network uses radio resource management (RRM) software embedded in every controller to analyze the over-the-air packets and alert the administrator to many different types of threats, including rogue access points, rogue clients, ad hoc networks, and denial-of-service attacks. RRM also enables the Cisco Unified Wireless Network to avoid RF interference. Precise physical location mapping of the threat is provided by the WCS. IT administrators can then choose to employ over-the-air containment of the rogue access point, client, or ad hoc network if desired. Precise determination of whether a rogue is connected to the enterprise network is offered through two methods: Rogue Location Discovery Protocol and rogue detectors.

In general, Cisco's strategy is a proactive one of preventing threats, rather than just reacting to them. Cisco offers a database of wireless attack signatures; however, many attack tools can easily modify these signatures. While the Cisco Unified Wireless Network allows customers to create custom signatures, Cisco believes a permanent solution is a more effective use of IT resources. In this vein, through Cisco's role in the IEEE 802.11w standards body, Cisco is leading industry efforts to not only detect, but also prevent DOS attacks and penetration attempts. A prestandards version of this capability, management frame protection, is available today.

The Cisco Unified Wireless Network offers several wireless IPS deployment modes to meet the varying needs of the enterprise. Access points can be deployed to serve clients and scan for wireless threats, or deployed as dedicated air monitors only. This latter mode is particularly useful for branch offices or portions of a main enterprise campus without wireless LAN coverage to provide protection against wireless threats. Unlike overlay wireless IPS systems, the air monitors can be converted to functioning access points at a later point, significantly reducing total cost of ownership.



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, CCIIP, 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)