Secure Wireless Architectures for Federal Agencies

Executive Summary

Key Benefits of the Cisco Unified Wireless Architecture

The Cisco Unified Wireless Architecture can provide:

- Enhanced productivity and collaboration because employees and guest users can securely access data and business-critical applications from conference rooms, offices, and public spaces
- Reduced operational expenses through simplified network deployment and operations capabilities
- Streamlined, real-time, dynamic network management because staff can control hundreds or even thousands of wireless access points from a single management console
- Enhanced flexibility using wired and wireless solutions to shape the network around the organization's unique needs
- End-to-end FIPS security for every component of the wireless architecture

The Challenge

One of the most difficult challenges facing the federal government in general and defense agencies in particular is how to protect data in-transit across wireless networks, while allowing agencies to benefit from mobile computing. In April 2004, the Office of the Secretary of Defense (OSD) issued DoD 8100.2, entitled "Use of Commercial Wireless Devices, Services and Technologies in the Department of Defense (DoD) Global Information Grid (GIG)," a policy that set a range of requirements for wireless security. These included mandating that all agencies adopt a Layer 2 encryption policy and that the solution must meet specific Federal security certifications such as the National Institute of Standards Federal Information Processing Standards (FIPS) 140-2 and NIAP Common Criteria validation. The result was that federal agencies deployed a wide range of proprietary solutions, which had to be overlaid on existing networks.

In June 2006 the OSD issued supplementary guidance to its April 2004 directive. Entitled "Use of Commercial Wireless Local-Area Network (WLAN) Devices, Systems, and Technologies in the Department of Defense (DoD) Global Information Grid (GIG)," the new document mandated that 802.11i/WPAv2 must be the new standard for Layer 2 encryption and that user authentication must be enforced while still meeting the FIPS 140-2 cryptographic requirements. The policy also mandates data confidentiality, data integrity, user or device authentication, nonrepudiation, high availability, location-based services, and wireless intrusion detection capabilities.

In addition to these operational requirements, government agencies should consider business-level concerns. A secure wireless architecture should reduce an agency's total cost of ownership, leverage existing wired infrastructure, use a common set of access-point/sensor hardware, deliver investment protection, support future location-based services in a cost-effective way, and converge wired/wireless security. Cisco® provides the most complete solution today to meet all aspects of the DoD policy, while integrating wireless into the wired infrastructure and creating a secure, seamless, and consistent end-user experience.

The Cisco® Unified Wireless Architecture transparently integrates key controls and security technologies from both wired and wireless components. This creates a defense-in-depth security architecture—including policy-based security, attack mitigation, 802.1x user authentication and authorization, FIPS-validated 802.11i/WPAv2 using Advanced Encryption Standard (AES) for wireless data confidentiality and data integrity, fast secure roaming, and embedded wireless intrusion detection and prevention—in standards-based enterprise solutions, which provide agencies with long-term, cost-effective scalability and ease of deployment and the reliability that they have come to expect from their wired networks.

The Solution

The Cisco Unified Wireless Architecture is the industry's only unified wired and wireless solution that increases employee productivity, enhances collaboration, and improves responsiveness to customers while it helps organizations address in a cost-effective manner the security, deployment, management, and control issues that they face in implementing a large-scale enterprise WLAN. The solution is designed for corporate offices, hospitals, retail stores, manufacturing floors, warehouse environments, educational institutions, financial institutions, local and national government agencies, and any other entity in which mobile connectivity is needed.

Designed as a multiservice solution, the Cisco Unified Wireless Network supports general business applications like e-mail and Internet access and also supports specialized applications like mobile healthcare, inventory management, video surveillance, and asset tracking. In addition to these data-oriented applications, customers can—if organization needs require—implement services such as guest access, voice over WLAN, wireless intrusion detection and prevention, precise location tracking, and Network Admission Control (NAC).

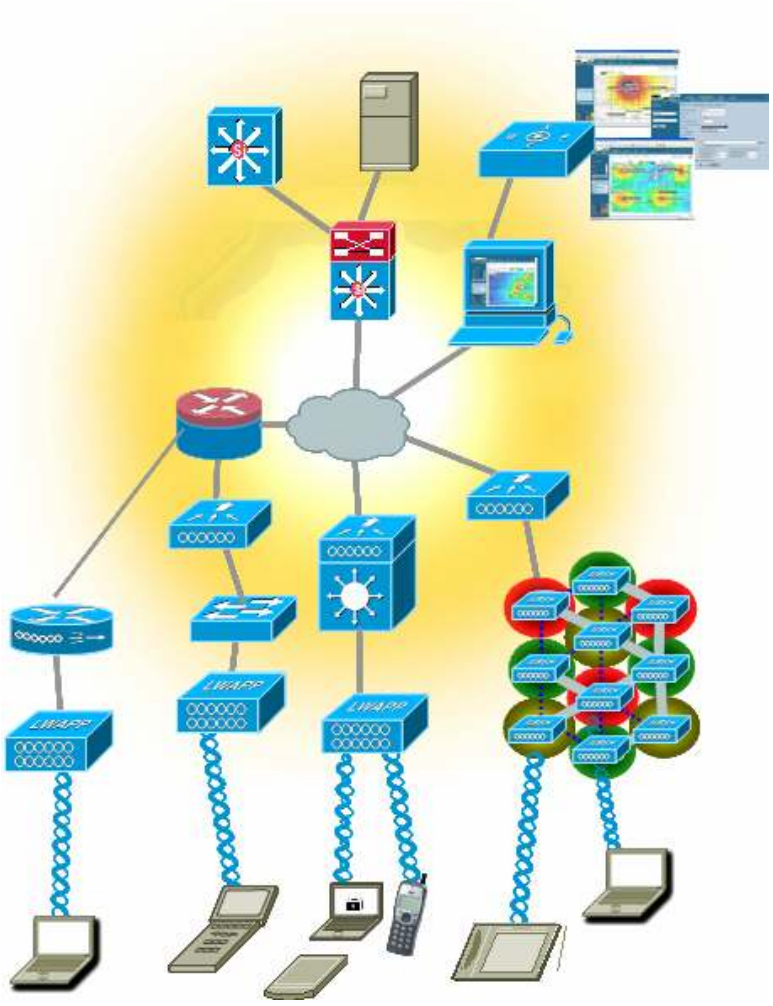
Based on industry standards (including IEEE 802.11 and the draft IETF CAPWAP standard), the Cisco Unified Wireless Network is an integrated, end-to-end solution that addresses all layers of the WLAN—from client devices and access points to network infrastructure, network management, advanced wireless services, and award-winning, worldwide, 24-hour product support. The Cisco Unified Wireless Network includes the following primary components:

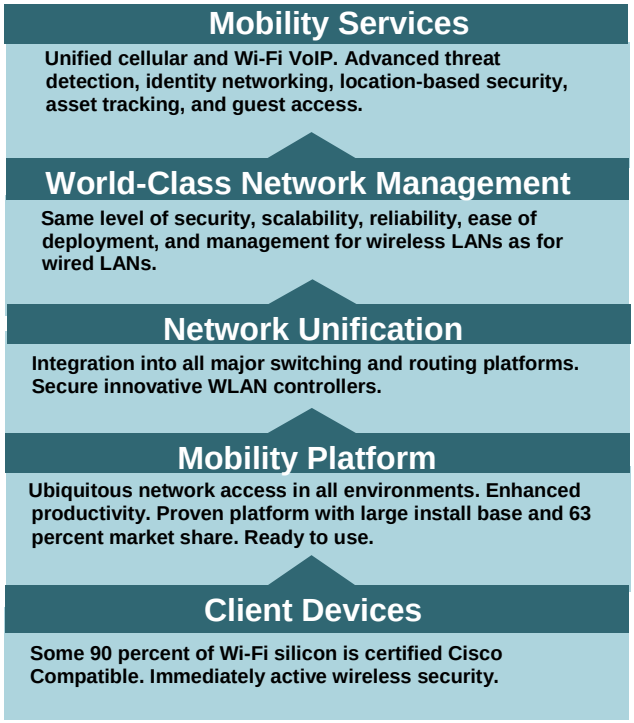
- Mobility services—The solution provides voice over wireless LAN (VoWLAN), advanced wireless intrusion detection and prevention, precise location tracking, guest access, and services for business-specific devices (point-of-sale, barcode scanning, and so on).
- World-class network management—The centralized management enables the same level of security, scalability, reliability, and ease of deployment as that of wired LANs.
- Wireless LAN controllers—Innovative centralized intelligence enables advanced services. Wireline network unification is achieved through integration into selected switching and routing platforms.
- Access points—Industry leading access points can be used in a variety of scenarios from indoor deployments to outdoor NEMA enclosure bridging/mesh solutions.
- Mobile clients—The solution serves a range of clients to meet business and security requirements. Some 90 percent of Wi-Fi silicon is certified Cisco Compatible, which assures peak performance and interoperability.

Based on years of customer experience and the largest install base in the industry, the Cisco Unified Wireless Network is the only integrated solution that addresses mobility services end to end throughout the WLAN—from the client to the application layer. Cisco always keeps in mind the critical role that the client plays in the network. To deliver industry-leading services such as

VoWLAN and RF identification (RFID), Cisco has embedded mobility into every layer of the network, which helps ensure that clients experience the reliability they expect from wired LANs. By enabling advanced features such as security, quality of service (QoS), and fast secure roaming in the client, Cisco can facilitate a consistent end-user experience.

Figure 1. Cisco Unified Wireless Network Architecture Enables Multiple Services





Return on Investment with Cisco

Operating budgets are tight, yet the market for WLANs is expanding. The reason is simple: wireless networking is a good investment. It increases productivity, decreases capital expense and operating costs, and makes a measurable positive impact on profitability. An NOP World study found that WLANs boosted employee productivity by an average of 22 percent. This increase comes from employees gaining the ability to check e-mail, schedule meetings, and access files and applications from conference rooms, classrooms, coworkers' desks, and virtually anywhere else within a building or campus.

Implementing a Cisco Unified Wireless Network can help an enterprise achieve the following positive results:

- Reduced total cost of ownership
- Increased employee collaboration
- Increased workforce mobility

Reduced Total Cost of Ownership

Total cost of ownership (TCO) is a critical component not just of commercial enterprise networks, but also of government applications, from the garrison to the soldier in the field. The Cisco Unified Wireless Network offers the following TCO savings:

Centralized management allows IT personnel to configure and manage the network from a wireless LAN controller, which in turn provides updates to all access points. This can translate to reduced expenditures for initial configuration and for ongoing software maintenance or upgrades. There can also be great savings in personnel time, if you assume that configurations or upgrades in networks that are not centrally managed will require an average of 20 minutes of personnel time per access point.

Unlike many systems that have independent networks for each communication function, the Cisco Unified Wireless Network enables voice, video, and data flow over a converged WLAN. This reduces the number of systems and devices, decreasing or eliminating the need for costly maintenance plans.

Because Cisco wireless architecture is based on industry standards, users can select best-in-class solutions to meet their unique RF requirements. The IETF Control and Provisioning of Wireless Access Points (CAPWAP) working group has selected the Lightweight Access Point Protocol (LWAPP) as the basis for the CAPWAP protocol. As this standard matures, the industry will see a reduction in the total cost of ownership and an increase in functionality and interoperability.

Cisco provides the industry's only integrated wireless network solution that incorporates intrusion detection, location services, and wireless client access. When planning a network, most vendors consider wireless to be an overlay architecture; intrusion detection and RFID capabilities are additional overlays. Cisco integrates its wireless technologies into the wired network and combines a wireless intrusion detection system (WIDS) and active RFID tracking in one solution. This unified solution significantly reduces both capital expenditures and operating expenses while it increases a mobile workforce's productivity.

Increased Collaboration

Organizations are increasingly being asked to do more with less, and wireless solutions can help by delivering increased opportunities for collaboration.

Employees on a Cisco Unified Wireless Network can save time by sending and receiving e-mail or accessing information on network servers from any meeting room or desk.

With a voice over WLAN solution, employees on a Cisco Unified Wireless Network can reach each other anywhere in the enterprise, without having to rely on cellular coverage that can be spotty or nonexistent.

Increased Workforce Mobility

The ability to respond rapidly to changing business conditions is critical in today's global economy, and the Cisco Unified Wireless Network can help.

Mobile workers can connect to the network quickly and easily at any local office to retrieve e-mail and receive voice communications without the IT staff having to do prior configuration. This can reduce the need for fixed office space and thereby lower costs.

IT personnel can add new locations or capacity more quickly with fewer resources. Centrally managed WLANs simplify network moves, adds, and changes. Temporary offices can be set up quickly with just a few access points and Wi-Fi enabled laptops.

Automatic RF management continuously senses changes in the WLAN coverage and helps address network disruptions by compensating for holes or dead spots as the RF environment changes.

Cisco Differentiators

Cisco is the global leader in WLAN solutions, with more than 63 percent of the market share for enterprise products. Acknowledged by Gartner Group as the Wireless LAN Magic Quadrant leader since 2003, Cisco delivers a comprehensive, unified wired and wireless solution. The importance of a unified solution has grown dramatically as WLAN deployments evolve from isolated areas that

support a few nonessential applications to enterprise wide, pervasive networks than run mission-critical applications like wireless VoIP and enterprise resource planning. The strength of Cisco WLAN solutions lies in the following areas.

Only Unified Wireless and Wired Solution

Pervasive WLAN deployment across the entire enterprise has propelled an evolution to integrate wireless-specific capabilities within the Layer 2 and Layer 3 wired infrastructure. Integrating this functionality uses the bandwidth, security, redundancy, and management capabilities of the network and provides a strong platform for expansion. Cisco is the first to introduce this next-generation WLAN solution with the Cisco Catalyst® 6500 Series Wireless Services Module (WiSM) and the Cisco Wireless LAN Controller Module for Cisco Integrated Services Routers.

Industry-Leading Security

As the number of wireless endpoints (laptops, personal digital assistants, smart phones, and so on) grows exponentially, securing the wireless network alone is insufficient to protect an enterprise. The corporate network is at risk from threats introduced through the wireless medium. Through IEEE 802.11i, wireless intrusion detection and prevention, and Cisco Network Admission Control (a key component of the Cisco Self-Defending Network Initiative), Cisco can both secure the wireless network and protect the corporate network against threats introduced by remote users, mobile workers, or wireless clients.

Feature-Richness and Standards

The Cisco Unified Wireless Network offers industry-leading features such as automatic RF management and multiple service levels for different user and client types, allowing differentiated QoS and security levels, VoWLAN, and location tracking for Wi-Fi devices and RFID tags. Cisco Unified Wireless Network services are built on a strong foundation of industry standards, including IEEE 802.11 and the forthcoming IETF CAPWAP. This means they will integrate easily with existing customer investments. For example, deployments that use the Cisco Catalyst 6500 Wireless Services Module take advantage of the powerful security, voice, and high availability capabilities of your existing infrastructure.

Where standards are not yet available, Cisco leads industrywide initiatives to enable new functionality that can be used in a multivendor environment. The Cisco Compatible Extensions program is one such area where new advances can be rapidly implemented and reach over 90 percent of the Wi-Fi client market.

Manageability and Scalability

Award-winning Cisco management allows up to thousands of access points to be configured and monitored. Automatic recognition of new access points results in correct configuration, helping to ensure that remote offices have the same security protocols as large campuses. Centralized management relieves network administrators of once manual tasks, enabling the WLAN network to scale to meet even large enterprise requirements.

Availability and Reliability

Cisco automatic RF management, wireless LAN controller clustering for redundancy, and intelligent network monitoring facilitate highly available WLAN solutions. If you experience a failure of WAN connectivity to remote branch offices, you can manage Cisco Unified Wireless Network solutions locally until the WAN link is repaired. Because Cisco Aironet® access points perform core

security functions and QoS processing locally, WAN links are not oversubscribed and customers get predictable and consistent levels of service.

Tested and Proven

Cisco testing labs help ensure that the end-to-end solutions of a Cisco Unified Wireless Network are manageable, scalable, available, and reliable. Using comprehensive Cisco design guides, network operators can easily and confidently implement and manage a Cisco Unified Wireless Network solution, as proven by the more than 70,000 Cisco customers using WLAN solutions and nearly 3 million Cisco access points deployed worldwide.

Conclusion

Cisco Unified Wireless Architecture is designed to support industry-leading mobility services in a state-of-the-art secure environment that improves the end-user experience as it delivers anytime, anywhere connectivity to employees using multiple media. This architecture offers a secure, scalable, flexible, and easily managed solution that can help you meet your business goals. With our extensive WLAN experience, Cisco can help extend the value of your network through WLAN solutions that improve employee productivity, enhance customer satisfaction, lower costs, and increase your business adaptability.

Technical Overview

Wireless networking technology has had a positive impact on many businesses over the past few years. It has provided mobility for clients, decreased the cost of connectivity in remote areas, and improved productivity in retail markets, where wireless technology has been used widely in point-of-sale applications. Many government agencies have not enjoyed these benefits due to the inherent security weaknesses in wireless technology as standards were being created. Over the past few years, improvements to the 802.11 protocol have increased WLAN security, beginning with the unsecure Wireless Equivalence Privacy (WEP), the Wi-Fi Protected Access (WPA), and, finally in June 2004, the IEEE ratified 802.11i (WPAv2), which set the new standard for wireless security.

Three key federal policies and guidelines set the parameters for designing secure enterprise wireless architectures. They are:

- DoD 8100.2—“Use of Commercial Wireless Devices, Services and Technologies in the Department of Defense (DoD) Global Information Grid (GIG)”
- DoD 8100.2—“Use of Commercial Wireless Local-Area Network (WLAN) Devices, Systems, and Technologies in the Department of Defense (DoD) Global Information Grid (GIG)”
- NIAP Common Criteria—“U.S. Government Wireless Local Area Network (WLAN) Access System Protection Profile for Basic Robustness Environments”

The first document, issued by the Office of the Secretary of Defense, mandated the use of strong authentication, nonrepudiation, and personal identification in accordance with DoD public key infrastructure (PKI). It also stated that encryption of wireless traffic via an assured channel was mandatory and must be FIPS140-2-validated. Finally, it mandated wireless intrusion detection, denial of service mitigation, and active screening for wireless devices.

In June 2006 the DoD issued the second document as supplementary guidance to DoD 8100.2. This document mandated that 802.11i/WPAv2 must be the new standard for Layer 2 encryption

and user authentication must be achieved by using the Extensible Authentication Protocol Transport Layer Security (EAP-TLS).

The third document, the Protection Profile targeted commercial wireless systems in a low-threat environment, called for layered security solution to mitigate attacks on the WLAN, and specified security and functional requirements of the system as whole and not individual components. It also required FIPS 140-2-approved encryption.

The Cisco Unified Wireless Architecture addresses federal wireless policies and certification requirements while providing a robust, feature-rich, integrated, low-cost solution. The FIPS-certified 802.11i architecture represents a paradigm shift from earlier deployments, which opens the door for federal agencies to benefit from the economies of standards-based networking.

In order to secure every aspect of enterprise wireless architectures, security mechanisms must be present at various layers throughout the network. Encryption of data in transit only ensures privacy—not end-to-end security. Cisco addresses WLAN security by offering multiple layers of protection, including the following:

- RF Security—Detects and avoids 802.11 interference and controls unwanted RF propagation
- WLAN intrusion prevention and location—Detects and locates rogue devices or potential wireless threats, which helps IT administrators to quickly assess the threat level and take immediate action to mitigate threats
- Identity-based networking—Enables enterprises to deliver individualized security policies to wireless users or groups of users with different access rights, device formats, and application requirements. The security policies include:
  - Layer 2 security—802.1X (PEAP, LEAP, TTLS), WPA, 802.11i (WPA2), 802.11w
  - Layer 3 (and above) security—Integration with wired intrusion prevention systems (IPS)
  - Access control lists—IP restrictions, protocol types, ports, and differentiated services code point values
  - QoS—Multiple service levels, bandwidth contracts, traffic shaping, and RF usage
  - Authentication, authorization, and accounting/RADIUS—User session policies and rights management
- Network Admission Control (NAC)—Enforces policies pertaining to client configuration and behavior to help ensure that only end-user devices with appropriate security utilities can gain access to the network
- Secure mobility—Maintains the highest level of security in mobile environments with Cisco Proactive Key Caching, an extension to the 802.11i standard and precursor to the 802.11r standard that facilitates secure roaming with Advanced Encryption Standard (AES) encryption and RADIUS authentication

With its multilayered approach to security, the Cisco Unified Wireless Architecture can be divided into components that address three critical tasks:

- Controlling client access
- Ensuring client integrity
- Protecting the network

Controlling Client Access

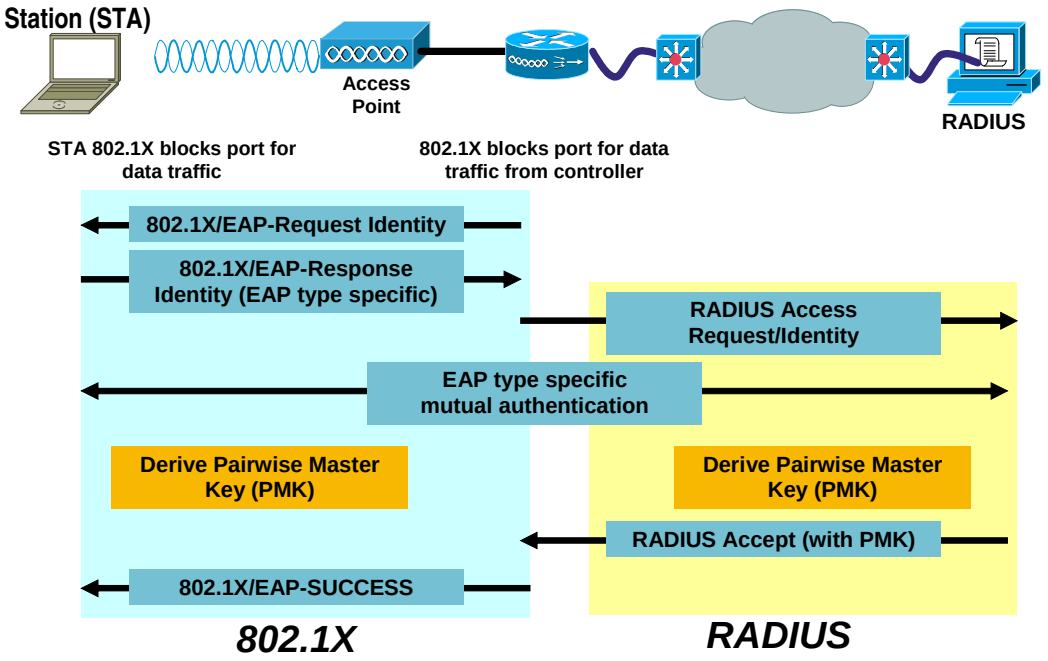
Given the new policies and guidelines on security, especially the recent mandate for the 802.11i standard, what must federal agencies do to make sure their wireless networks are secure? The first and most important step is to control client access. To accomplish this, a wireless network must ensure confidence through proper client authentication and data encryption.

Authentication

Network access control is the cornerstone of security for federal wireless architectures. Access to the wireless medium must be restricted and users must be authenticated. The IEEE 802.1x standard is used as the transport mechanism for user- or machine-based authentication. It is a standard for media-level access control, offering the capability to permit or deny network connectivity, control VLAN access, and apply traffic policy. The 802.1x protocol is not part of the set of 802.11 wireless standards; instead it describes a standard link-layer protocol used for transporting higher-level authentication protocols. Three critical pieces interact in 802.1x authentication: the Supplicant (client) that resides on the wireless end device, the Network Access Server (WLAN controller), and the Authenticator (Cisco Secure Access Control Server). No network traffic can flow from the client to the network until a successful authentication occurs. Prior to authentication, the client cannot obtain an IP address, therefore any login scripts or additional authentication mechanisms that require IP connectivity will be unsuccessful until the authentication is complete. In a FIPS-validated architecture, the 802.1x supplicant, Access Point, Wireless LAN Controller must also be FIPS 140-2 certified.

As part of the adoption of the 802.11i standard, the Extensible Authentication Protocol (specified in RFC 3748) must be used to transport client authentication. Originally designed for use with the Point-to-Point Protocol (PPP [RFC 1661]) EAP has been adapted to 802.1x based networks. The EAP message carries authentication information in the 802.1x packet. Several EAP methods are available, including EAP-TLS, Protected EAP (PEAP) and EAP-Flexible Authentication via Secure Tunneling (EAP-FAST).

Figure 2. EAP Authentication Overview



The June supplement to DoD 8100.2, which set 802.11i as the new standard for Layer 2 encryption, also specified the use of EAP-TLS in accordance with DoD policy for mutual authentication using PKI. EAP-TLS (specified in RFC 2716) is an authentication protocol that uses TLS, providing cipher suite (cryptographic parameters) negotiation, mutual authentication, and key management capabilities. In EAP-TLS, PKI-issued digital certificates are used to authenticate the supplicant to the authentication server, and, optionally, to authenticate the authentication server to the supplicant.

The authentication server starts by sending its digital certificate to the supplicant. Today, Secure Sockets Layer (SSL) is the most common authentication method used on the Web. It is a one-way authentication—a server sends its certificate to your browser to prove its identity. However, EAP-TLS uses mutual authentication to protect your network against man-in-the-middle attacks.

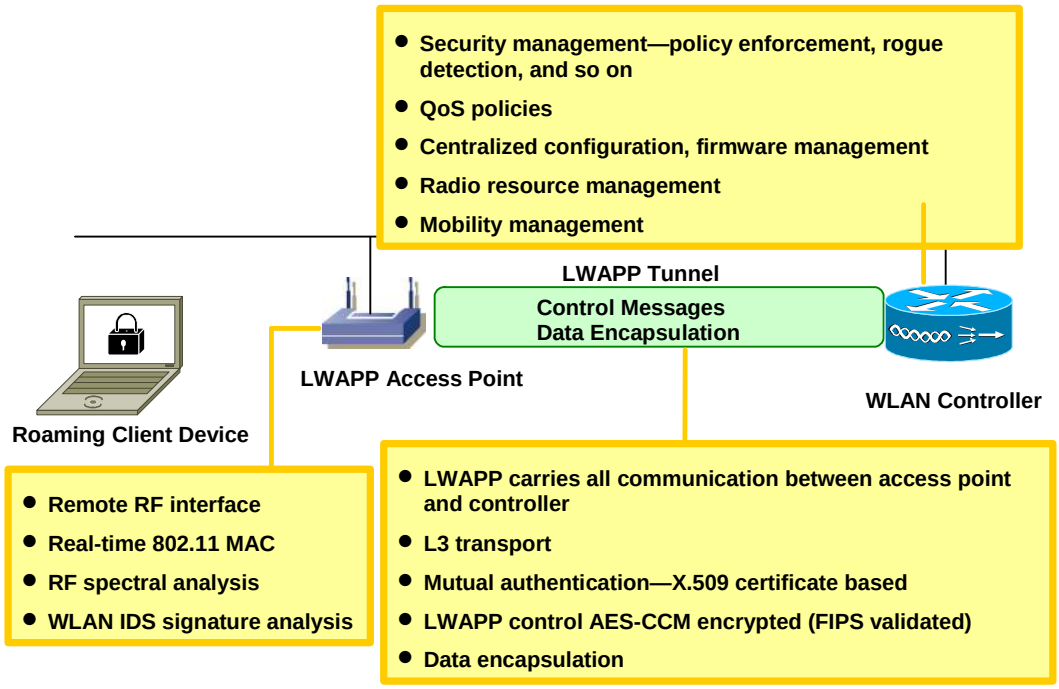
Finally, TLS has achieved FIPS 140-2 validation, certifying that the TLS protocol meets federal encryption standards to securely encrypt and transport authentication messages.

Two methods of authentication may be used when deploying EAP-TLS in conjunction with 802.1x to establish a secure wireless environment: client certificates and/or machine certificates. In most cases the X.509 certificate used for the EAP-TLS authentication is supplied by a Smart Card or Common Access Card (CAC). To better communicate the impact of EAP-TLS on DoD deployments, Appendix A provides a brief overview of CAC or Smart Card use for PKI authentication. Depending on the deployment requirements, both client and machine certificates are acceptable forms of Identification to provide access to the network.

Encryption

The cornerstone of Cisco Unified Wireless Architecture is the LightWeight Access Point Protocol (LWAPP). LWAPP is defined by an IETF RFC draft document which is the basis for the IETF CAPWAP working group. The CAPWAP working group will ultimately produce an industry standard wireless control protocol, but for now LWAPP is the most mature protocol available. Appendix B contains additional information on the details of LWAPP. Not only is the wireless data-in-transit encrypted, but all phases of the of the initial authentication process are secured using FIPS-validated encryption algorithms using AES 128-bit keys. All user traffic from the client station to the access point (AP) is encrypted in accordance with the 802.11i specification; the LWAPP command and control channel used between the AP and the wireless LAN controller (WLC) to distribute configuration information is encrypted and FIPS validated; and all RADIUS traffic between the WLC and the RADIUS server is encrypted using the RADIUS key wrap protocol (specified in the IETF draft zorn-radius-keywrap-10). This end-to-end security approach protects all aspects of the EAP authentication, access point configuration and 802.11i encryption key distribution. This uniquely enables Cisco to provide a defense-in-depth security framework that precludes the possibility of the compromise of a single device to allow access to the rest of the network.

Figure 3. Cisco Secure Wireless Architecture's end-to-end security approach



Data In-Transit Encryption—802.11i

Once a wireless network has authenticated a station or user, it is critical to ensure that the data cannot be hijacked or compromised in transmission over that network. The best way to guard the integrity of data over the air is through the use of standards based encryption technologies. This area of wireless security is the primary focus of the 802.11i standard. The 802.11i specification mandates the use of AES in Counter mode with CBC-MAC (AES-CCM) 128-bit keys to ensure the integrity of the data in transmission, provisions for Temporal Key Integrity Protocol (TKIP) as part of the 802.11i standard, were added for backward compatibility. When operating in a FIPS validated mode, TKIP must be disabled due to the use of the RC4 encryption algorithm which

cannot be FIPS validated. AES-CCM uses authenticated-encryption modes, including a counter for confidentiality and CBC for authenticity with a single key. It also relies on cipher block chaining message authentication code (CBC-MAC) for authentication and integrity and replay protection, and provides 64-bit message integrity check (MIC), an improvement over TKIP's 20-bit MIC. The IEEE 802.11i specification provides the most robust Layer 2 security for federal agencies while meeting FIPS 140-2 requirements, being standards-based and facilitating vendor interoperability.

Control Plane Encryption

The LWAPP control plane is protected by the mutual authentication of devices during the process of the AP's initial connection to the WLC and by encryption of the control message payload of all LWAPP control messages. The LWAPP control message payloads are encrypted using industry standard FIPS 140-2 validated AES-CCM algorithm.

As a basis for explaining how the LWAPP control plane is protected, we must first establish these key facts:

- The AP and WLC have X.509 certificates burned into protected flash.
- The X.509 certificates are signed by a private key that is burned into the devices at the time of manufacture. Both the AP and WLC have the appropriate public encryption keys installed.
- The AP and WLC have certificates installed that allow them to trust the issuing certificate authority (of the AP or WLC certificate).

When the AP sends a join request to the WLC, it embeds its X.509 certificate in the LWAPP message. It also generates a random session ID and includes it in the LWAPP join request. When the WLC receives the LWAPP join request, it validates the signature of the X.509 certificate using the AP's public key and checks that the certificate was issued by a trusted certificate authority. It also looks at the starting date and time for the AP certificate's validity interval and compares that date and time to its own date and time. If the X.509 certificate is valid, the WLC generates a random AES encryption key. WLC next encrypts the key using the AP's public key, concatenates the resulting ciphertext with the session ID in the join request, and encrypts the concatenated value using its own private key. The WLC copies the results into the LWAPP join response along with its own X.509 certificate. When the AP receives the LWAPP join response, it validates the WLC certificate signature using the WLC's public key and checks that the certificate was issued by a trusted certificate authority. If the WLC certificate is validated, the AP extracts the encrypted key portion. It decrypts the concatenated ciphertext using the WLC's public key and validates the session ID. It then decrypts the AES key using its private key.

The AP maintains a key lifetime timer. When the timer expires, the AP generates a new session ID and embeds it in an LWAPP key update request message to the WLC. The WLC repeats the previously described key generation and distribution process and embeds the new ciphertext in an LWAPP key update response. The key lifetime timer is eight hours.

Authentication/Radius Encryption

In 2001, the NIST published a draft AES key wrap specification describing a NIST-approved encryption protocol that would be used to transport sensitive cryptographic keying material. Following that, a proposal for a secure means of key delivery using RADIUS attributes and the AES key wrap algorithm was created and is currently under review as an IETF draft.

RADIUS key wrap support is essentially an extension of the RADIUS protocol, providing a FIPS certifiable means for a Cisco Secure ACS to authenticate RADIUS messages and distribute session keys. As RADIUS is used to transport EAP messages (in the EAP-Message attribute), securely authenticating RADIUS messages will simultaneously provide for securely authenticated EAP message exchanges.

RADIUS key wrap is used for secure delivery of the 802.11i pairwise master key (PMK) from an 802.1X Authentication Server (Cisco Secure Access Control Server [ACS]) to a network access server (NAS), e.g., a wireless LAN controller. The WLC will then derive the per-user session key or Pair Wise Transient Key (PTK) and deliver that to the appropriate Access Point via the FIPS validated LWAPP encrypted control channel. Simultaneously, the FIPS validated WLAN client will generate a PMK from information obtained during the EAP authentication process—and then generate per-session PTK. At no time during the authentication process is any cryptographic keying material transmitted in an unprotected manner more specifically, keying material (PMK or PTK) is never transmitted over the 802.11 network to the client.

Ensuring Client Integrity

To ensure a client's integrity, a network must be able to deal with the problems inherent in mobile computing, especially mobile workers who may use their computers to access the network from unsecured locations. As previously described, a secure network must protect data integrity and prevent unwanted access. It must also be able to report anomalous behavior on the client and by the client.

Installing strong antivirus protection and personal firewalls on a mobile device is the traditional method of keeping a client safe. But a secure network should also use a host-based intrusion detection system (IDS) that can determine both misuse (malicious or abusive activity inside the network) and intrusion (breaches from outside the network).

Host-Based IDS

A host-based IDS should provide inbound and outbound port blocking, protection from fragmented packet attacks, and protection from attacks using "evasion" techniques. It should also have configurable IDS rules, application execution protection, and location-aware protection.

Aside from infecting endpoints, viruses and worms frequently create network congestion as a byproduct of rapid propagation. Cisco began addressing both problems by offering its customers an endpoint intrusion prevention called the Cisco Security Agent. Cisco Security Agent uses novel forms of behavioral security to detect viruses and worms, prevent them from gaining a foothold on an endpoint system, and prevent them from propagating across a network. In effect, Cisco Security Agent becomes a first-order dampener to the virus and worm propagation effect.

A second and equally compelling reason for deploying Cisco Security Agent is that it establishes a presence on endpoints that can be used to establish a feedback loop between the endpoint and the network, resulting in a network that rapidly adapts to emerging threats. Cisco Security Agent provides threat protection for server and desktop computing systems. It aggregates multiple security functionality, combining host intrusion prevention, distributed firewall, malicious mobile code protection, operating system integrity assurance, and audit log consolidation—all within a single agent package. As part of an overall strategy, Cisco Security Agent enables the end-to-end security approach that adds to our defense-in-depth architecture.

As high-visibility network security attacks like Code Red and the SQL Slammer worm have shown, traditional host and desktop security technologies have limited capability to combat the effects of new and evolving attacks. Unlike traditional signature-matching security technologies, the Cisco Security Agent analyzes behavior to provide robust protection with reduced operational costs. By identifying and preventing malicious behavior before it can occur, Cisco Security Agent removes potential known and unknown (“Day Zero”) security risks that threaten enterprise networks and applications.

Network Admission Control

In addition to controlling client access through the use of 802.1X, a secure wireless network must perform periodic posture assessment and remediation services for wireless users. Periodically validating the integrity of the client through posture assessments helps ensure that the network enforces end point compliancy with the appropriate critical security patches, virus software, and security policies for the mobile device prior to granting it access. If a device is found to be noncompliant, the network can enforce security policies by blocking, isolating, and repairing noncompliant machines. The machines are redirected into a quarantine area, where remediation occurs at the discretion of the administrator.

The following key security features are provided to help ensure the client’s integrity:

- Web login authentication, adopting one or more authentication servers such as RADIUS, Kerberos, LDAP, NTLM, etc.
- Custom splash Web page, distinctively unique per managed subnet, VLAN, or operating system
- Layer 3/Layer 4 role-based access control (RBAC) to permit access to specific port, protocol, or subnet
- Bandwidth throttling for each user role by assigning shared or dedicated bandwidth usage
- Guest session timeout management such as 2 hours for visitors and 24 hours for employees
- Custom URL redirection to a predefined page for acceptable user policy notice
- Preconfigured Windows critical hot fixes and antivirus application checks
- Self-remediation for quarantined users

Protecting the Network

To protect the network, federal agencies must have a defense-in-depth architecture that uses a multilayered security approach. Security architectures should include three critical components: wireless intrusion detection systems (WIDS), location services, and the upcoming IEEE 802.11w standard for management frame protection (MFP).

Wireless networks use WIDS to detect and contain rogue access points and clients and to scan for 802.11-based attacks. The systems must be able not only to track a rogue device but also to pinpoint its location, determine whether it is launching an attack, and remove it from the network as quickly as possible. Intelligent off-channel scanning can quickly detect rogues and ad hocs.

Location services have also proved valuable in rogue client detection and containment. These services effectively track clients as they enter a wireless network. They also make the wireless network more transparent, by providing answers to four key questions:

- What do we have?
- How many do we have?
- Where are they?
- What is their status?

Location services provide another level of control on the client by allowing access based on physical location. For example, client access to the wireless network can be cut off as soon as the client leaves a defined area.

One limitation of wireless IDS/IPS is that it will detect only wireless denial-of-service (DoS) attacks, providing no protection against valid authenticated users that may inadvertently launch a Layer 3 IP DoS attack. Cisco has taken a comprehensive approach to creating a unified security architecture by integrating its wired and wireless security systems. When the Cisco Unified Wireless Architecture is deployed with a Cisco wired IPS device, the IPS device will detect any associated client devices that are sending malicious Layer 3 traffic through the network. The wired IPS device will then send a shun request to the wireless LAN controller. This effectively blocks/disassociates the client device at the edge of the network, extending your security control to the perimeter.

An emerging wireless standard, 802.11w, will provide management frame protection (MFP). MFP secures the management frame communications between a client and an AP by appending all frames with authenticated, signed MAC (AES hashed message authentication code [HMAC]). It protects clients from a wide range of attacks and security risks created by the open nature of management frame communications used in 802.11. As a result, anomalies are detected instantly and reported.

The Cisco pre-802.11w implementation is titled Management Frame Protection (MFP). It provides security features for the otherwise unprotected and unencrypted 802.11 management messages passed between access points and client stations.

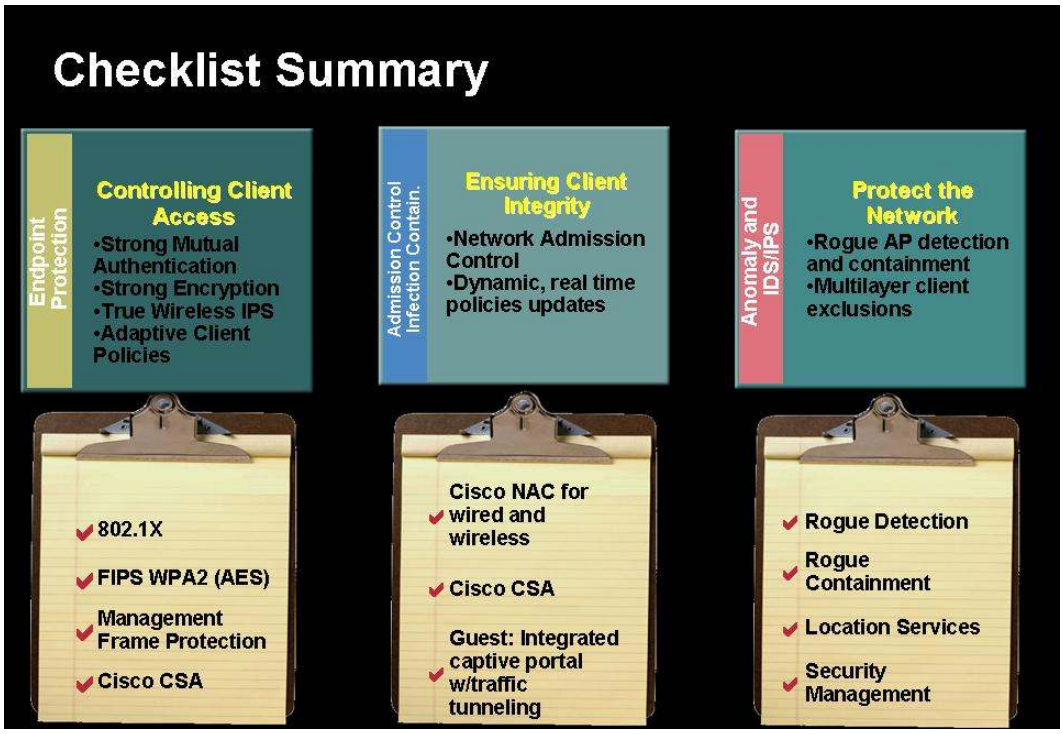
MFP comprises the following two functional components:

- Infrastructure support
- Client support

Infrastructure support provides quick and accurate detection of spoofing events. When coupled with signed beacons, it provides an effective means to detect and report phishing, the latest mode of attack on WLANs. This protects 802.11 session management functions by adding MIC information elements to the management frames emitted by access points (not those emitted by client stations), which are then validated by other access points in the network.

Client support shields authenticated clients from spoofed frames, preventing many of the common attacks against WLANs from becoming effective. Most attacks (deauth attacks, etc.) revert to just degrading performance by contending with valid clients. This encrypts management frames sent between APs and MFP-capable client stations so that both the AP and client can take preventive action by dropping spoofed management frames (i.e. those passed between an AP and a client

station that is authenticated and associated). By applying AES-CCM in a manner similar to that used for data frames, the network can protect management frames.



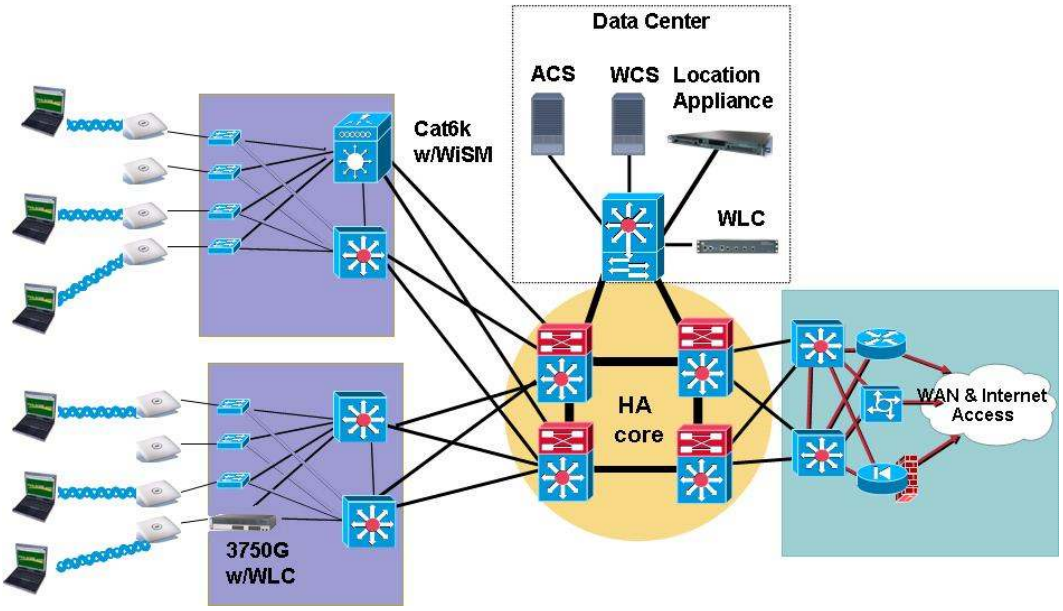
Architecture Design

There are three key components of the Cisco Unified Wireless Architecture that must meet FIPS validation requirements. Two other components used for wireless intrusion detection and prevention are required for WLAN architecture submitted to NIAP for Common Criteria certification.

- FIPS validated wireless LAN controller (WLC)
- FIPS validated access points
- Cisco Secure Access Control Server (RADIUS server)
- Wireless intrusion detection/intrusion prevention
  - Wireless control software
  - Location appliance

The placement of access points and controllers within the enterprise architecture can follow typical campus WLAN deployments guidelines and recommendations (see Figure 4).

Figure 4. Typical campus WLAN deployment guidelines



Architecture Components

Wireless LAN Controllers

Cisco wireless LAN controllers are responsible for systemwide WLAN functions, such as integrated intrusion prevention, real-time RF management, zero-touch deployment, and N+1 redundancy. There are three form factors of FIPS validated WLCs that can be deployed on the network, depending upon the current Layer 2/Layer 3 infrastructure requirements.

- The Cisco Catalyst 6500 Series Wireless Services Module—The Cisco WiSM integrates seamlessly into networks that have deployed Cisco Catalyst 6500 Series Layer 3 switches with the Supervisor 720. The WiSM provides industry-leading security, mobility, redundancy, TCO savings, and ease-of-use for large-scale WLANs. It is designed for medium-sized and large enterprise facilities with clustering capabilities of up to 3600 lightweight access points per roaming domain. It scales to 300 lightweight access points per module with support for more than 10,000 wireless client devices.

Cisco Wireless Services Module

- The Cisco Catalyst 3750G Integrated Wireless LAN Controller—This Cisco WLC delivers secure, enterprise wireless access to midsize organizations and branch offices requiring support for 50 to 200 lightweight access points in one logical unit. A logical unit is a stack of up to nine 3750G switches. The Cisco Catalyst 3750G Integrated Wireless LAN Controller delivers centralized security policies, wireless IPS capabilities, award-winning RF management, QoS, and Layer 3 fast secure roaming. As a core component of the Cisco Unified Wireless Network, the Cisco Catalyst 3750G Integrated Wireless LAN Controller provides the control, security, redundancy, and reliability that managers need in order to scale and manage their wireless networks as easily as they do their wired networks.

Cisco Catalyst 3750G Integrated WLC

- The standalone Cisco 4400 Series wireless LAN controller—This WLC fully integrates with the network infrastructure to deliver enhanced security features, enforce QoS polices, and deliver other advanced services. The capacity of the 4000 Series WLC ranges from 12 access points up to 100 access points. These controllers can be clustered together to provide support for up to 2400 access points per roaming domain.

Cisco 4400 Series WLC

Access Points

Two series of Cisco Aironet lightweight access points meet the criteria for FIPS 140-2 validation and fall in line with the DoD 8100.2 policy. Both the 1130 AG and the 1240 AG access points offer secure, manageable, and reliable wireless connectivity with exceptional capacity, range, and performance. They support a wide array of deployment options, including single or dual radios, integrated or external antennas, and rugged metal enclosures. Cisco Aironet access points deliver the versatility, high capacity, security, and enterprise-class features demanded by WLAN customers. These access points come standard with ready-to-use wireless features for “zero-touch” configuration. Both series can be completely managed by Cisco wireless LAN controllers and the Cisco Wireless Control System (WCS), which centralizes key functions of WLANs to provide scalable management, security, and mobility between indoor and outdoor deployments.

- The Cisco Aironet 1130 AG Series—This access point packages high capacity, high security, and enterprise-class features, delivering wireless LAN access for a low total cost of ownership. Designed for wireless LAN coverage in offices and similar RF environments, this unobtrusive access point features integrated antennas and dual IEEE 802.11a/g radios for robust and predictable coverage, delivering a combined data rate of 108 Mbps.
- The Cisco Aironet 1240 AG Series—This IEEE 802.11a/b/g access point offers the same enterprise-class features as the 1130 AG but is designed for RF environments that require the antenna versatility associated with connectorized antennas, a rugged metal enclosure, and a broad operating temperature range.

Cisco Aironet 1130 AG Series and Cisco Aironet 1240 AG Series Access Points

AP 1130 and AP 1240

Cisco Secure Access Control Server

The Cisco Secure Access Control Server (ACS) is a high-performance and highly scalable user and administrative access control solution that operates as a centralized RADIUS or TACACS+ server system. In the context of 802.11i, Cisco Secure ACS plays a critical role in authenticating users to the network via multiple EAP methods (EAP-TLS, PEAP, and EAP-FAST) and is also responsible for the 802.11i PMK generation used for individual per-user session keys required by 802.11i. The Cisco Secure ACS is the first RADIUS server to be submitted to NIST for FIPS validation of the RADIUS key wrap protocol. As previously described, the RADIUS key wrap protocol will protect the RADIUS traffic between the WLC and ACS to provide a FIPS-approved method for key distribution.

Wireless Intrusion Detection/Prevention With Location

Using the wireless medium, unauthorized persons can now perpetrate a wide variety of new threats on an enterprise. Rogue access points are the most common, but other threats include MAC spoofing attacks, client misconfiguration, and denial-of-service attacks. To combat these attacks, the Cisco Unified Wireless Network supports advanced wireless intrusion detection and prevention services. With this capability, the network can automatically identify attacks in real time, as they happen. For rogue access points, a dual over-the-air and wireline suppression strategy is implemented. Clients that try to associate with the rogue access point are automatically blocked, without harming the operation of authorized WLAN access points. Using information collected both over the air and on the wired side, Cisco can automatically initiate port suppression and further disable the rogue access point from passing traffic to the wireline. Precise location tracking is the final step that enables the physical removal of the rogue device.

Wireless Control Software

The Cisco Wireless Control Software works in conjunction with Cisco Aironet lightweight access points, Cisco wireless LAN controllers, and the Cisco Wireless Location Appliance. With Cisco WCS, network administrators have a single solution for RF prediction, policy provisioning, network optimization, troubleshooting, user tracking, security monitoring, and wireless LAN systems management. Robust graphical interfaces make wireless LAN deployment and operations simple and cost-effective. Detailed trending and analysis reports make Cisco WCS vital to ongoing network operations. When used in conjunction with the Cisco Wireless Location Appliance, WCS is an essential component of the Cisco wireless architecture’s intrusion detection and prevention.

Wireless Location Appliance

The Cisco Wireless Location Appliance plays an integral part in the tracking of rogue APs and clients throughout the WLAN. It tracks location through the use of advanced RF fingerprinting technology, simultaneously tracking thousands of 802.11 wireless devices from directly within the

WLAN infrastructure, thus increasing asset visibility and control of the air space. The Cisco Wireless Location Appliance also records rich historical location information that can be used for location trending, rapid problem resolution, and RF capacity management.

WIDS—WCS + Location

The Cisco Wireless Intrusion Detection System has 17 standard WIDS signatures, which it uses to detect rogue devices (access points and clients) and other hostile or threatening activity. Once the Cisco Aironet access points are powered up and associated to the WLAN controllers, they scan the coverage area 24 hours a day for the presence of rogue APs, rogue clients, and suspect wireless traffic that may be operating within the environment. As the controller detects intrusions, it generates real-time alerts that the WCS management console immediately updates. The controllers also dispatch alarm notifications to administrators with further details about the offending activity.

Together, the APs, controllers, and WCS components provide location capabilities for tracking the physical location of a single rogue AP or rogue client device that may be detected. When the Cisco 2700 Series Wireless Location Appliance is added, the system can tracking the physical location of thousands of wireless devices—including rogue APs and rogue clients—in real time. The location appliance also provides the WCS with on-demand location tracking history for tracking the physical movement of RFID tags or any single device within the environment. The WCS compares RSSI signal strength from one, two, or more access points and analyzes RF fingerprinting algorithms to find the most probable location of rogue AP and rogue clients. Once it detects a rogue, the WCS places a unique rogue icon directly on the map of the coverage area displaying its most likely location.

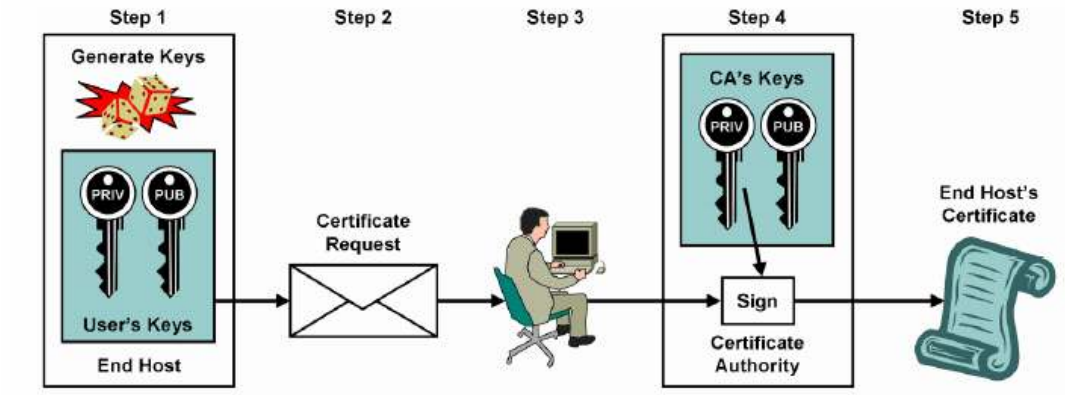
The WIDS and location-tracking functionalities are integrated directly into the system, thus providing simultaneous WLAN data distribution services and WIDS services. The system does not require dedicated monitor APs, but it can be set into dedicated monitor mode if desired. In monitor mode, the AP acts as an overlay wireless monitoring system, but without any WLAN data services being transmitted. This mode can be used to enforce a “no wireless” policy for wired-only networks. In both modes of operation (WLAN service or dedicated monitor mode), the WIDS functionality provides containment capabilities that give administrators the ability to manually disallow wireless communications by any device on the wireless network. Containment services can be performed by one, two, or three APs associated to a controller.

Appendix A: DOD Public Key Infrastructure and Common Access Cards

Public Key Infrastructure Overview

Public key infrastructure (PKI) offers a scalable method of securing networks, reducing management overhead, and simplifying the deployment of network infrastructures by deploying security protocols, including IP Security, Secure Shell, and Secure Sockets Layer. PKI manages encryption keys and identity information for the human and mechanical components of a network that participates in secured communications. For a person or a piece of equipment to enroll in a PKI, the software on a user's computer must generate a pair of encryption keys—a public key and a private key—that will be used in secured communications. In the case of the Common Access Card (CAC), the keys and certificates are stored on the CAC smart card. The private key is never distributed or revealed. Conversely, the public key is freely distributed to any party that negotiates a secure communication. During the enrollment process (as shown in Figure 1), the user's public key is sent in the certificate request to the Certification Authority (CA), which is responsible for the portion of the organization to which that entity belongs. The user sends the public key to the registration component of the CA. Subsequently, the administrator approves the request and the CA generates the user's certificate. After the user receives a certificate and installs it on the computer, he or she can participate in the secured network. For CACs, this entire process is handled when the CAC is provisioned.

Figure 1. Public Key Infrastructure Enrollment



The identity components determine the identity of the user, the user's level of access to the particular type of communication under negotiation, and the encryption information that protects the communication from parties who are not allowed access. Communicating parties will exchange certificates and inspect the presented information. The certificates are checked to see if they are within their validity period and if the certificate was generated by a trusted PKI. If all the identity information is appropriate, the public key is extracted from the certificate and used to establish an encrypted session.

Detailed documentation on PKI is readily available on the Internet or in numerous publications.

CAC Components

The CAC provides two-factor authentication. To unlock the certificates on the CAC, the user must place the physical CAC in a reader and enter a personal identification number (PIN). This unlocks the private keys stored on the CAC. The private keys are never exported or placed on the workstation.

CAC Reader

The CAC Reader is an International Standards Organization (ISO) 7816 standard Smart Card Reader. The user must place the CAC into the reader in order for the information on the card to be read. Drivers must be installed on the PC in order for the CAC to be read by another piece of software, called middleware.

Middleware

The user interface to the CAC is the middleware installed on the workstation. The middleware prompts the user for the PIN, unlocks the CAC, and provides all communications between the operating system and the CAC Reader. Typical middleware is ActivCard Gold for CAC, Datakey Middleware for CAC, Netsign CAC, and so on. The communication between the CAC middleware and the Windows operating system (OS) occurs through the Microsoft Certificate Application Programming Interface (CAPI). Using CAPI, the middleware presents the certificates to the OS. Any applications that use the CAPI can access the certificates.

Appendix B: LWAPP Overview

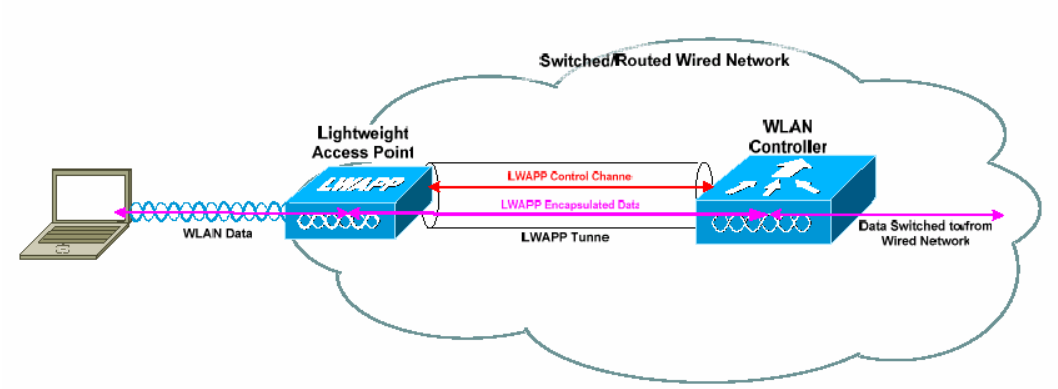
The Cisco Unified Wireless Architecture centralizes WLAN configuration and control on a device called a wireless LAN controller (WLC). This allows the WLAN to operate as an intelligent information network and to support advanced services, unlike the traditional 802.11 WLAN infrastructure, which is built from autonomous, discrete entities. The Cisco Unified Wireless Network architecture simplifies operational management by collapsing large numbers of managed endpoints, autonomous access points, into a single managed system of WLAN controller(s). In this architecture, access points are lightweight, meaning that they cannot act independently of a WLC. The WLC manages the AP configurations and firmware. The APs are “zero-touch” deployed, and no individual configuration of access points is required. The APs are also lightweight in the sense that they handle only real-time MAC (media access control) functionality, leaving the WLC to process all the non-real-time MAC functionality. This is referred to as split-MAC architecture. As Figure 1 shows, APs interact with the WLAN controller via the Lightweight Access Point Protocol (LWAPP). LWAPP defines the following:

- Control messaging protocol and format
- Data encapsulation

WLAN client data packets are encapsulated in LWAPP between the AP and the WLC. WLCs forward data frames to and from WLAN clients after encapsulating or de-encapsulating the frames. When a WLAN client sends a packet, the AP receives it, decrypts it if necessary, encapsulates it with an LWAPP header, and forwards it to the controller. At the controller, the LWAPP header is stripped off and the frame switched from the controller onto a VLAN in the switching infrastructure. When a client on the wired network sends a packet to a WLAN client, the packet first goes into the WLC, where it is encapsulated with an LWAPP header and forwarded to the appropriate AP. The AP strips off the LWAPP header, encrypts the frame if necessary, and then bridges the frame onto the RF medium.

LWAPP control messages are encrypted using the industry standard FIPS validated AES-CCM encryption method. The shared encryption key is derived and exchanged when the AP joins the WLC. The payloads of encapsulated LWAPP data messages are not specially encrypted. A trusted wired network is assumed and standard best practices for protecting networks should be followed. Standards-based FIPS validated 802.11i wireless Layer 2 encryption is handled at the access point.

Figure 1. APs interact with WLAN controller via LWAPP



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.**

Printed in USA

C11-390657-00 03/07