# Guide to Secure and Agile Wireless Solutions for the Federal Market

## Contents

## What You Will Learn

As interest in and use of wireless local area networks (WLANs) among businesses and consumers throughout the world have grown, the utility and cost-effectiveness of wireless technologies have been acknowledged within governments as well. Following the strengthening of wireless technology standards to ensure greater security and reliability, the U.S. government has issued various guidelines and directives for federal agencies interested in deploying WLANs. An overview of these are presented in this paper, along with a description of the Cisco® Unified Wireless Network architecture, associated technologies, and products, which are designed to adhere to the most stringent of government standards for federal agencies, including those issued by the U.S. Department of Defense (DoD).

## Overview

Wireless networking technology has been extremely beneficial for many organizations by improving operational efficiencies. It has provided mobility for users, improved employee productivity and decreased the cost of providing network connectivity. Until recently, many government agencies have not enjoyed these benefits due to security concerns and lack of policy concerning the deployments of WLANs. But these attitudes are changing, with the availability of 802.11i (WPA2 Enterprise), security agencies within the U.S. federal government are now increasingly deploying wireless local area networks (WLANs) for employees. More recently, Cisco has taken a leadership role in the development of the 802.11ac standard, which is a faster and more scalable version of 802.11n. It couples the freedom of wireless with the capabilities of Gigabit Ethernet, achieving an increase in speed through more channel bonding, denser modulation, and more spatial streams.

A February 2012 report by Market Research, Ltd., reports that government wireless data traffic is now doubling on an annual basis and reached the level of voice traffic in 2011. The report forecasts that the U.S. government wireless voice and data market will grow at a compound annual growth rate (CAGR) of 14 percent by 2018, reaching $17 billion in expenditures.

A 2010 report by the U.S. Government Accountability Office (GAO) touted the advantages of wireless technology for federal workers, including increased flexibility, easier installation, easier scalability than wired networks, and the ability of workers with wireless devices to securely connect to an agency network through a public Internet access point or hot spot while traveling. Younger employees are used to mobile devices and social networking applications, and thus expect ubiquitous access through WLANs. To attract and retain these workers, the government has determined that it must make wireless access a priority.

Government agencies often work with highly confidential information whose release may prove damaging to national security, foreign and domestic policy, economic stability, and agency and individual reputations. Thus, the need for the reliable security of WLANs in the federal government has prompted the drafting of policies, standards, and requirements that agencies are mandated to follow.

The government's adoption of the Federal Information Processing Standards (FIPS) validated IEEE 802.11i standard has led to widespread WLAN deployments throughout many government agencies, including the DoD. Despite this growth, there is still lingering skepticism in some agencies about the ability of WLAN security technologies and standards to maintain confidentiality for sensitive information. Yet, as more and more government users realize the significant benefits of wireless mobility and understand how to certify their WLANs and receive DoD Information Assurance Certification and Accreditation Process (DIACAP) 'Authority to Operate,' this reluctance to deploy WLANs in government will lessen.

**Certifications applicable to the Cisco Unified Wireless Network (UWN)**

FIPS

Cisco APs and WLAN Controller are fully FIPS validated.

Unified Capabilities (UC) Approved Products List (APL)

The Cisco UWN is listed on the DoD UC APL.

Unified Capabilities Requirements (UCR)

Cisco UWN meets the requirements of the UCR.

Joint Interoperability Test Command (JITC)

The Cisco UWN has been fully evaluated by JITC.

DoD Information Assurance Certification and Accreditation Process (DIACAP)

The Cisco UWN through the DIACAP process for multiple DoD customers.

DISA STIGs

The Cisco UWN fully complies with the requirements of the DISA STIGs.

Common Criteria

Common Criteria is a certification, move this to the certifications category and change title to

Cisco UWN is Common Criteria Certified.

## Cisco Unified Wireless Network

The Cisco Unified Wireless Network addresses federal wireless policies and certification requirements while providing a robust, feature-rich, integrated, low-cost solution. The FIPS-validated 802.11i architecture represents the first certified wireless solution that can enable federal agencies to deploy wireless LANs to provide the same services as their wired LANs.

A secure wireless architecture must reduce an agency's total cost of ownership (TCO), take advantage of existing wired infrastructure, use a common set of access-point and sensor hardware, deliver investment protection, support future location-based services in a cost-effective way, and converge wired and wireless security and policies. Cisco provides the most complete solution today to meet all aspects of federal government policies, while integrating wireless into the wired infrastructure and creating a highly secure, seamless, and consistent end-user experience.

The Cisco Unified Wireless Network transparently integrates key controls and security technologies from both wired and wireless components. This creates:

- 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, highly secure roaming
- Embedded wireless intrusion detection and prevention

The Cisco Unified Wireless Network can provide government agencies with long-term, cost-effective scalability and ease of deployment, as well as the reliability that they have come to expect from wired networks.

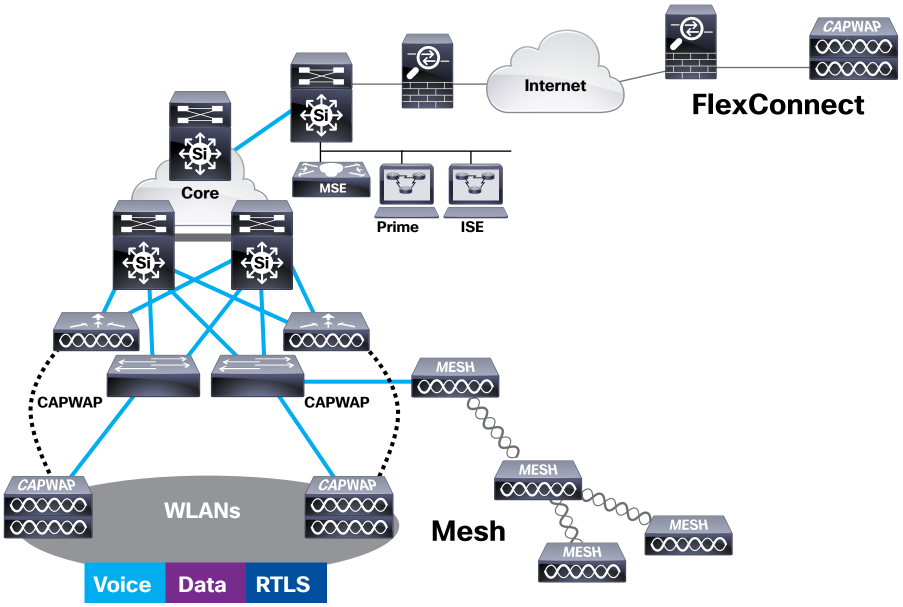
The Cisco Unified Wireless Network is made up of five major components:

- Lightweight access points provide the wireless connectivity to the mobile clients and can forward all 802.11 MAC layer communications to the Wireless LAN Controller.
- Wireless LAN Controller (WLC) centrally manages the configuration of all the lightweight access points. The WLC also serves as the MAC layer bridge, bridging 802.11 Ethernet traffic to 802.3.
- Network management is available in two varieties: the Cisco Wireless Control System (WCS) and Cisco Prime™ Infrastructure.
- Wireless services are delivered through the Cisco Mobility Services Engine (MSE). The Cisco MSE provides a location tracking feature called Context Aware Mobility Solution, and an enhanced wireless intrusion prevention system (IPS) capability called Adaptive Wireless IPS (wIPS). The MSE also plays a key role in delivering Cisco CleanAir® capabilities.
- Authentication Server – Cisco offers two FIPS-validated authentication servers: the Cisco Access Control System (ACS) and the Cisco Identity Services Engine (ISE). Either option will provide robust authentication services. Furthermore, ISE adds profiling and guest services that are becoming a necessity for the enterprise.

Guidelines and policies for WLANs in federal government agencies

- DoD Instruction 8100.2
- DoD instruction 8420.01
- National Information Assurance Partnership (NIAP)
- Guidelines for Securing WLANs issued by NIST

Figure 1. Cisco Unified Wireless Network Architecture



Based on IEEE 802.11 and CAPWAP (RFC 5415) standards, the Cisco Unified Wireless Network is an industry-leading unified wired and wireless solution that can increase employee productivity, enhance collaboration, and improve 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 email 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 bring your own device (BYOD), guest access, voice over WLAN (VoWLAN), wireless intrusion detection and prevention, and precise location tracking.

The Cisco Unified Wireless Network was developed based on years of customer experience and has achieved the largest install base in the industry to date. It is the only integrated solution that addresses mobility services end to end throughout the WLAN–from the client to the application layer. To deliver industry-leading services such as VoWLAN and Wi-Fi-based radio frequency identification (RFID), Cisco has embedded mobility into every layer of the network, which ensures that clients experience the same reliability they expect from wired LANs. By enabling advanced features such as security, quality of service (QoS), and fast, highly secure roaming in the client, Cisco offers a consistent end-user experience.

Cisco also is currently the only networking vendor that has 802.11ac-ready wireless infrastructure. Upgrading Cisco Aironet® 3600 Series Access Points to be 802.11ac-capable is quick and easy with an extension module.

## Mobility Services

WLAN security is a requirement for all federal government agencies. Cisco Context Aware Mobility Solution can provide organizations with the ability to see what devices are accessing their wireless network. Network threat detection and mitigation is another important requirement for WLANs that is addressed with the Cisco Adaptive wIPS. The emerging Hotspot 2.0 standard, a specification created by the Wi-Fi Alliance and championed by Cisco, will make it easier for mobile users to join and roam among public Wi-Fi networks. These three technologies are described below.

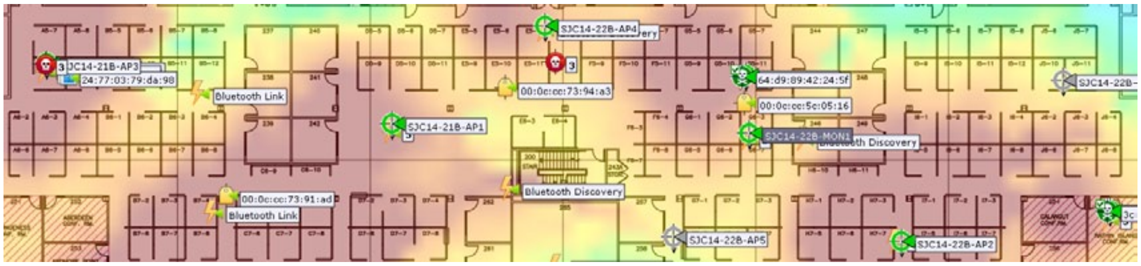
### Cisco Context Aware Mobility Solution

Cisco Context Aware Mobility Solution allows organizations to quickly locate rogue devices, interferers, Wi-Fi clients, tagged assets, and wired devices. Knowledge of the physical location of assets provides the insight needed to improve workflow, quickly troubleshoot mobile clients, and implement asset management solutions.

The detailed location information is provided through an open API, which can enable applications such as:

- Asset management, to provide real-time visibility into the location, status, and movement of equipment throughout the organization
- Process optimization, to increase efficiency and safety, and to save both employee and customer time
- Integration with a wide range of tags capable of providing telemetry information such as temperature monitoring of sensitive assets

Figure 2. Context Aware service provides location tracking of clients, RF-ID tags, rogues and interferers.



Cisco Context Aware Mobility Solution provides real-time and historical information on the health of the wireless network and the physical location of assets, rogue devices, and interferers. This information empowers network administrators to quickly and easily troubleshoot wireless problems. It also increases visibility to collect critical business intelligence and to monitor traffic patterns so that the WLAN can be optimized to provide the best experience to end users.

With the Cisco Context Aware Mobility Solution, mobile users can go beyond anytime, anywhere connectivity to automatically use the best device, the best application, and the best environment while on the go. The service allows for tracking and location-awareness of IP-enabled devices, both wired and wireless, within the Cisco Unified Wireless Network and wired network. Wireless devices include Wi-Fi-enabled client devices and Wi-Fi-active RFID Cisco Compatible Extension (CCX) tags. Wired devices include any IP-enabled wired device that connects to a Cisco Catalyst® switch.

Another benefit of Cisco Context Aware Mobility Solution is that it maintains the location history of all Wi-Fi assets, including rogue devices. This can greatly enhance the ability of administrators to troubleshoot wireless issues based on historical records.

### Cisco Adaptive wIPS

The Cisco Adaptive wIPS is integrated within the Cisco Unified Wireless Network infrastructure and provides wireless-specific network threat detection and mitigation against malicious attacks, security vulnerabilities, and sources of performance disruption. Cisco Adaptive wIPS provides the ability to detect, analyze, and identify wireless threats, and can centrally manage mitigation and resolution of security and performance issues. Cisco Adaptive wIPS also delivers proactive threat prevention capabilities for a hardened wireless network core that is impenetrable by most wireless attacks, allowing customers to maintain constant awareness of their RF environment to minimize legal liability, protect brand reputation, and assure regulatory compliance, including PCI 2.0 standards.

Cisco Adaptive wIPS embeds complete wireless threat detection and mitigation into the wireless network infrastructure to deliver a superior, comprehensive, accurate, and operationally cost-effective wireless security solution. Some key functions it performs include:

- Rogue access point, client, and ad hoc connection detection and mitigation
- Over-the-air wireless hacking and threat detection
- Security vulnerability monitoring
- Performance monitoring and self-optimization
- Network hardening for proactive prevention of threats
- Complete wireless security management and reporting

These features encompass DoD security policies for the most stringent WLAN environments.

Passpoint

Cisco has over 40 products Passpoint certified.

Passpoint is the Wi-Fi alliance Brand name for Hotspot 2.0.

### Hot Spot 2.0

Hotspot 2.0 is a Wi-Fi Alliance device certification program and technical specification designed for Wi-Fi clients and infrastructure devices to support seamless connectivity to Wi-Fi networks. The Hot Spot 2.0 specification is based on the 802.11u specification, which enhances network discovery and selection by Wi-Fi clients. It also draws on the 802.1x/EAP architecture. With the finalization of the Hotspot 2.0 specification the Wi-Fi Alliance has introduced the Passpoint brand name.

The specification will provide back-end integration between infrastructure such as WLAN controllers and access points, and hub AAA proxy servers, operator AAA servers, and user databases. It also provides protocols and components that allow clients to learn about back-end devices on wireless networks (for example, what service providers or roaming partner agreements are available through the basic service set [BSS], and what the hotspot service model is like). Greater back-end transparency facilitates the seamless client selection and connectivity process.

## Key Cisco Technologies for WLAN Quality and Efficiency

### Cisco CleanAir Technology

CleanAir technology is a systemwide feature of the Cisco Unified Wireless Network that can simplify operations and improve wireless performance by providing complete visibility into the wireless spectrum. CleanAir technology has the unique ability to perform spectrum analysis and detect RF interference that other systems cannot see. It can identify the source, locate it on a map, and then make automatic adjustments to optimize wireless coverage.

Cisco CleanAir technology is enabled by the advanced silicon design of the Cisco Aironet 3600, 3500, 2600, and 1600 Series Access Points, as well as by Cisco Wireless Controllers, the Cisco Wireless Control System (WCS), Cisco Prime Infrastructure, and the Cisco Mobility Services Engine. The technology uses silicon-level intelligence to create a spectrum-aware, self-healing, and self-optimizing wireless network that mitigates the impact of wireless interference and offers performance protection for 802.11n networks.

Cisco CleanAir technology enables organizations with the ability to:

- Automatically optimize the wireless LAN for better reliability and performance
- Perform remote troubleshooting for fast problem resolution and minimum downtime
- Detect non-Wi-Fi security threats and resolve issues in real time with CleanAir Analyst, allowing non-Wi-Fi interference to be mapped in real time with existing network resources
- Monitor air quality for the entire installation 24 hours daily and generate alerts on customizable anomalies
- Monitor and track historic interference information for back-in-time analysis and faster problem solving with CleanAir Analyst
- Set and enforce policy with intelligent identification of non-Wi-Fi devices

Cisco CleanAir technology is enabled through dedicated hardware, using ASIC technology, to offload the ability to detect and classify interferers without impacting access point performance. By freeing the CPU from these tasks, this ensures that the access point can perform its primary job of processing and passing wireless communications.

### Cisco ClientLink Technology

Cisco ClientLink technology helps improve the link quality of wireless devices, including 802.11a and g, so that clients connect at higher data rates and more efficiently utilize the airwaves. Unlike most 802.11n access points, which only improve uplink performance, Cisco ClientLink improves performance on both the uplink and the downlink, providing an improved user experience during web browsing, email, and file downloads. ClientLink technology is based on signal processing enhancements to the access point chipset and does not require changes to network parameters.

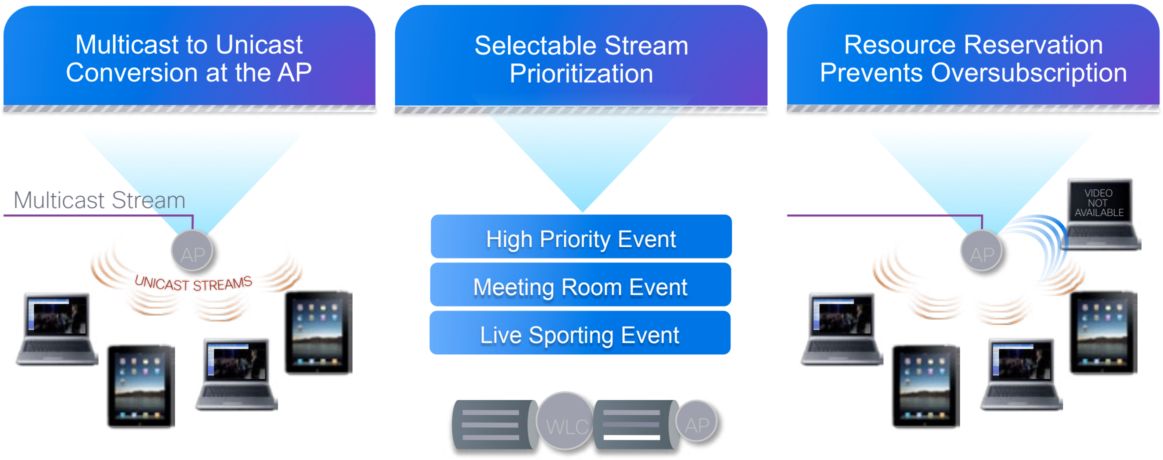
ClientLink beamforming integrates advanced signal processing into the wireless chipset. ClientLink uses multiple transmit antennas to focus transmissions in the direction of the client. It can enable the access point to optimize the signal-to-noise ratio (SNR) exactly at the position where the client is placed. Improved SNR yields many benefits, such as a reduced number of retries and higher data rates. By allowing the wireless system to operate at higher data rates and with fewer retries, ClientLink increases the overall capacity of the system, which means more efficient use of spectrum resources. This technology does not depend on any client-side hardware or software capabilities; and is compatible with 802.11a, .11g and .11n client devices.

ClientLink can improve coverage areas between cells or near obstacles and can ensure airtime “fairness” so that all clients, regardless of location or version of the 802.11 standard, have the optimal connection to the Cisco wireless network. Through the use of ClientLink, Cisco wireless network can improve the spectrum efficiencies by up to 25 percent.

### Cisco VideoStream Technology

Cisco 802.11n products extend the high-definition video experience to Wi-Fi networks. Cisco VideoStream technology optimizes the way video is delivered through the wireless infrastructure. Using Cisco’s RF and video expertise, VideoStream can deliver reliable, consistent, high-quality video performance to the client without creating a burden on the network.

Figure 3. Video stream optimizes rich media traffic delivery through the use of multicast, traffic prioritization and resource reservation control.


Multicast to Unicast Conversion at the AP
Selectable Stream Prioritization
Resource Reservation Prevents Oversubscription
Multicast Stream
AP
UNICAST STREAMS
High Priority Event
Meeting Room Event
Live Sporting Event
WLC
AP
AP
VIDEO NOT AVAILABLE

Cisco VideoStream technology can enable the wireless infrastructure to:

- Assign stream prioritization to any stream at up to eight priority levels. This helps to ensure high-quality and consistent delivery of critical video applications
- Manage admission and policy control with Resource Reservation Control for bandwidth protection and channel optimization against additional requests causing oversubscription
- Increase the reliability of video stream delivery by converting multicast video streams to unicast at the access point
- Efficiently use the wired network by utilizing the multicast version of CAPWAP. Through the capabilities of multicast, the wired network will distribute the multicast CAPWAP data stream to only the access points that have clients requesting the video stream

Cisco VideoStream provides clear, accurate video images everywhere by efficiently delivering multicast video from the wired to the wireless network. VideoStream technology maintains video quality at a perfect 5.0 medium opinion score (MOS) score. It can deliver three times the scalability of competing products and can optimize network performance by using 30 times less bandwidth than competing products.

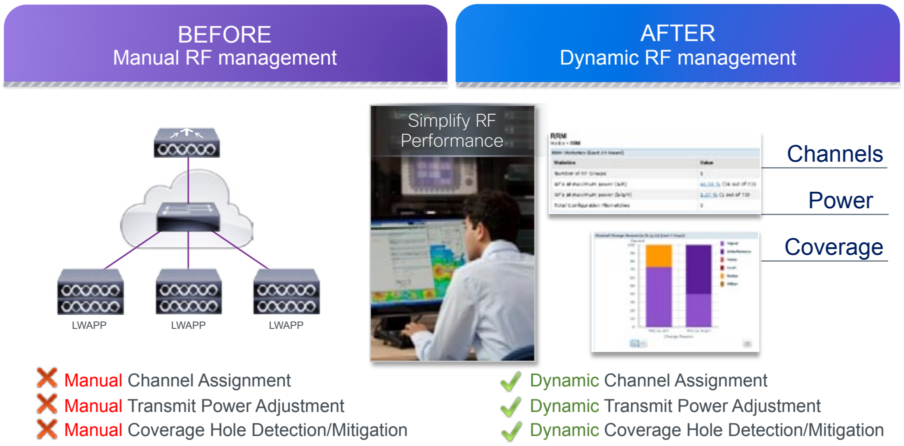
### Band Select

The 2.4-gigahertz (GHz) band is often congested. Clients on this band typically experience interference from Bluetooth devices, microwave ovens, and cordless phones as well as co-channel interference from other access points because of the 802.11b/g limit of three non-overlapping channels. Band Select counters these sources of interference and improves overall network performance by encouraging client radios that are capable of dual-band (2.4 and 5 GHz) operation to move to a less congested 5-GHz access point.

### Radio Resource Management (RRM)

The 802.11 specification was originally architected primarily with a home, single-cell use in mind. The contemplation of the channel and power settings for a single access point was a trivial exercise, but as pervasive WLAN coverage became a key user expectation, determining each access point’s settings necessitated a thorough site survey. Thanks to the shared nature of 802.11 bandwidth, the applications that now run over the wireless segment are pushing customers to move to more capacity-oriented deployments. The addition of capacity to a WLAN is an issue unlike that of wired networks where common practice is to throw more bandwidth at the problem. Additional access points are required to add capacity, but if they are improperly positioned and/or configured, interference and other factors can actually decrease the capacity of the wireless network.

Figure 4. RRM automatically selects and optimizes channel and output coverage to provide the ideal coverage.


BEFORE
Manual RF management
AFTER
Dynamic RF management
LWAPP
LWAPP
LWAPP
Simplify RF Performance
RRM
Channels
Power
Coverage
✗ Manual Channel Assignment
✗ Manual Transmit Power Adjustment
✗ Manual Coverage Hole Detection/Mitigation
✓ Dynamic Channel Assignment
✓ Dynamic Transmit Power Adjustment
✓ Dynamic Coverage Hole Detection/Mitigation

As large-scale, dense WLANs have become standard, administrators are continuously challenged with these RF configuration issues that can increase operating costs. If handled incorrectly, these issues can lead to WLAN instability and a poor end-user experience.

With finite spectrum (a limited number of non-overlapping channels) to play with, and given RF's innate desire to bleed through walls and floors, designing a WLAN of any size has historically proven to be a daunting task. Even given a flawless site survey, RF is ever-changing and what might be an optimal access point channel and power schema at one moment may prove to be less than functional the next.

Cisco RRM allows the Cisco Unified WLAN architecture to continuously analyze the existing RF environment, automatically adjusting the power levels of access points and channel configurations to help mitigate such things as co-channel interference and signal coverage problems. RRM can reduce the need to perform exhaustive site surveys, increase system capacity, and provide automated self-healing functionality to compensate for RF dead zones and access point failures.

## Cisco Unified Wireless Network Security Solutions Overview

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:

- Highly secure wireless infrastructure – Cisco utilized the IETF standard CAPWAP protocol to help ensure that all components of the Cisco Unified Wireless Network, access points, and controllers are fully authenticated, and that all control and management traffic is encrypted and secured
- Radio frequency (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 – Can enable 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 (EAP-TLS, EAP-FAST and EAP-PEAP), 802.11i (WPA2), 802.11w
    - Layer 3 (and above) security – Integration with wired IPS access control lists (ACLs) – 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
- Secure mobility – It is paramount to maintain voice and video communications across a highly mobile environment. The Cisco implementation of Fast Secure Roaming, including 802.11r, can ensure that highly mobile devices maintain WPA2 enterprise-secured communications while delivering seamless roaming and mobility throughout the enterprise

The Cisco Unified Wireless Network can be divided into components that address three critical tasks:

- Assured wireless infrastructure
- Controlling and securing client access
- Protecting the network

## Assured Wireless Infrastructure

In order for the Cisco Unified Wireless Network to provide highly secure wireless communications it must first ensure that all aspects of the wireless infrastructure are secured. This includes:

- Helping to ensure that only trusted access points are allowed to connect to the wired network
- Utilizing a standards-based protocol for the provisioning and control of the wireless infrastructure
- Ensuring that only trusted access points are allowed to connect to the WLAN controllers
- Highly secure management of the wireless infrastructure
- Highly secure distribution of keying material from the authentication server to the access point

### Ensuring That Only Trusted Access Points Are Allowed on the Wired Network

To prevent rogue access points from accessing the wired network, when an access point is connected to a switch that supports 802.1x, the access point acts as an 802.1x supplicant and must be authenticated by the switch. If successfully authenticated, the access point can then attach to the wired network and establish a connection to the WLC.

Furthermore, if a Cisco Identity Service Engine (ISE) is deployed across the network, it can act as the authentication server. ISE will profile the connected endpoint to ensure that it is a Cisco access point. If the connected endpoint does not match the profile of a Cisco access point, it will not be allowed to connect to the network.

### Standards-based Provisioning and Control of the WLAN

The cornerstone of the Cisco Unified Wireless Network is the CAPWAP protocol. The CAPWAP protocol is defined by IETF RFC 5315 and is the protocol used for all communication between the lightweight access points and the WLAN controller. The protocol defines the use of two tunnels or planes per access point connection to the WLAN controller: the CAPWAP control plane and the CAPWAP data plane.

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

The access point and the WLC use x.509 certificates that are burned into protected flash memory as the credentials to establish the secure CAPWAP control plane. Once an access point successfully connects to the wired network, it attempts to locate the WLAN controller. The most common method for the access point to locate the controller is through the use of an option 43 during the DHCP process. The access point attempts to associate to the WLAN controller but before it can associate to the controller it must first authenticate. The access point and the controller utilize the hardware certificates to perform a mutual authentication. Once authenticated, the access point establishes a FIPS 140-2 validated AES-CCM DTLS control tunnel to the WLAN controller. All management traffic to the access point traverses this control plane, helping to ensure that the access point cannot be hijacked by an intruder on the wired network. Cisco also provides customers with the ability to use their own trusted PKI environment. Customers can add their own Locally Significant Certificates (LSCs) to their WLAN infrastructure, thus ensuring that only their trusted access points will associate to their controllers.

WPA2 Enterprise

Wi-Fi alliance link for definition

### Highly Secure Management of the Wireless infrastructure

The Cisco Prime Infrastructure is made up of three primary components: the Oracle database engine, a web server engine, and a Java-based Simple Network Management Protocol (SNMP) engine. All three components work together to provide the complete management functionality. The web server provides highly secure SSL access to the management console. As an added level of security, customers can install their own x.509 certificates to be used for secure HTTPS access. The SNMP engine on the Cisco Prime Infrastructure is used to communicate with the WLC. SNMP is used to push the configurations to the WLC and to gather configurations, logs, and traps. To provide the most secure form of management, Cisco Prime Infrastructure uses SNMPv3. Version 3 encrypts SNMP packets to help ensure privacy. It provides an authentication mechanisms to help ensure messages are from a trusted source, and integrity to help ensure packets have not been tampered with.

### Secure Distribution of Keying Material

Client authentication occurs between the supplicant (running on the client device) and an authentication server like Cisco Secure Access Control Server (ACS) or Cisco ISE. This communication passes through the access point and the WLC to the authentication server. The WLC serves as the authenticator and will require information from the authentication process to establish secure 802.11i communication to the wireless client. Steps must be taken to ensure this keying material is securely transferred to the WLC.

RADIUS key wrap support, an extension of the RADIUS protocol, provides a FIPS-certifiable means for a Cisco ACS or a Cisco ISE to authenticate RADIUS messages and more securely distribute session keys. RADIUS key wrap is used for secure delivery of the 802.11i pairwise master key (PMK) from an authentication server to a network authenticator (the WLC). The WLC will then derive the per-user session key or Pairwise Transient Key (PTK) and deliver that to the appropriate access point using the FIPS-validated, CAPWAP-encrypted control channel. Simultaneously, the FIPS-validated WLAN client will generate a PMK from information obtained during the EAP authentication process and then generate a per-session PTK. At no time during the authentication process is any cryptographic keying material transmitted in an unprotected manner (for example, keying material–PMK or PTK–is never transmitted over the 802.11 network to the client).

## Controlling and Securing Client Access

Given the federal government’s policies and guidelines on security, especially the mandate for the 802.11i standard, federal agencies must take a variety of steps to ensure that 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 authenticator (WLAN controller), and the authentication server (Cisco ISE or ACS). 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

**How Cisco provides FIPS-validated TLS:**

Cisco WLAN controllers are FIPS-validated for EAP-TLS when providing local EAP authentication

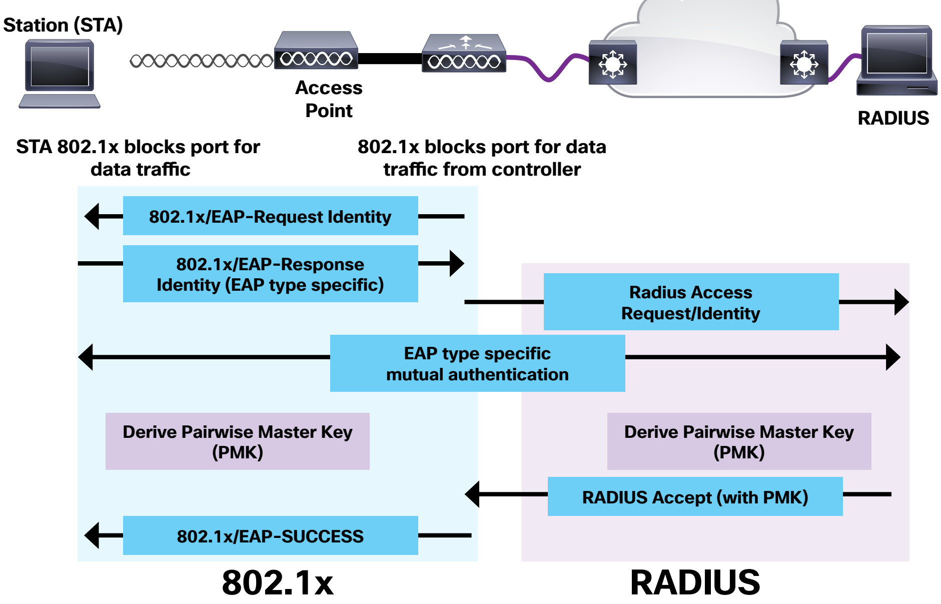
Cisco ISE 1.1 uses a FIPS-validated Cisco SSL, Cisco Common Crypto Module (C3M) (FIPS Cert. #1643)

The Cisco AnyConnect® Network Access Module (NAM) is FIPS validated for TLS (including EAP-TLS, EAP-PEAP, and EAP-FAST) through use of the FIPS-validated Cisco SSL C3M.

be unsuccessful until the authentication is complete. In a FIPS-validated architecture, the 802.1x supplicant, access point, WLAN controller, and authentication server must all be FIPS 140-2-validated.

As part of the adoption of the 802.11i standard, the EAP (specified in RFC 3748) must be used to transport client authentication. 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 outlines EAP authentication.

Figure 5. EAP Authentication Overview


Station (STA)
Access Point
RADIUS
STA 802.1x blocks port for data traffic
802.1x blocks port for data traffic from controller
802.1x/EAP-Request Identity
802.1x/EAP-Response Identity (EAP type specific)
Radius Access Request/Identity
EAP type specific mutual authentication
Derive Pairwise Master Key (PMK)
Derive Pairwise Master Key (PMK)
RADIUS Accept (with PMK)
802.1x/EAP-SUCCESS
802.1x
RADIUS

The DoD Instruction 8420.01 specifies the use of EAP-TLS in accordance with DoD policy for mutual authentication using PKI. EAP-TLS 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.

Two methods of authentication may be used when deploying EAP-TLS to establish a secure wireless environment: client certificates and 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) or personal identity verification (PIV) card. Depending on the deployment requirements, both client and machine certificates are acceptable forms of identification to provide access to the network.

When supporting Windows laptops, the most secure option would be to implement both machine and user authentication:

- As a laptop boots up, it automatically authenticates to the network using a machine certificate or other credential. The laptop is isolated to a network that will allow management through MS-SMS, Altiris, or another product. This will also allow for group policy administration before the user logs onto the system.
- When the user logs into Windows, the authentication server will be configured to enforce machine access restriction (MAR). MAR states that the client's MAC address must already be authorized in order for the user to log on to the machine. The laptop successfully authenticates to the WLAN with the user credentials and is connected to the enterprise network.
- The user then successfully authenticates to the domain and logs into Windows.

A real- world example is a laptop connected to a docking station. Docking stations provide the conveniences of a desktop while offering the portability of a laptop. When the laptop is docked, connectivity to the network goes through the wired connection. When the user undocks the laptop to attend a meeting, they expect to seamlessly connect to the WLAN and continue working. However, this does not work correctly because the user is already logged on to the laptop and when the (undocked) laptop attempts to authenticate to the network it uses the user credential and not the machine credential. The authentication server attempts to enforce MAR but it does not have any record of the wireless network interface card (NIC0 MAC address previously being authenticated so the user authentication fails. Thus, the user can no longer access the network.

To addresses the shortcomings of the separate machine and user authentication, Cisco has developed EAP Chaining. EAP Chaining allows for the passing of the machine credential with the user credential during a single EAP session. Therefore, in the above scenario, when the user removes their laptop from the docking station the user credential and the machine credential will be passed to the authentication server. From the user's perspective, network connectivity is seamlessly maintained. EAP Chaining is currently supported using the EAP-FAST authentication protocol. This requires version 3.1 of Cisco AnyConnect Network Access Module (NAM) supplicant and version 1.1.1 of the Cisco ISE Authentication Server.

Cisco AnyConnect NAM meets FIPS requirements and also provides the ability to enforce no access to the wireless network when connected to the wired network, a requirement for clients connecting to a DoD network. AnyConnect NAM also has the ability to require that users connect to the enterprise WLAN when it is present, thereby preventing wireless clients from accessing untrusted networks when in the enterprise. The foundation of NAM is AnyConnect, which can be used to secure remote connectivity so if users connect to an untrusted WLAN, the AnyConnect VPN can be used to ensure highly secure client communications.

### Data-in-Transit Security

All user traffic from the client station to the access point is encrypted in accordance with the 802.11i specification as mandated by most federal policies. 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 Cipher Block Chaining Message Authentication Code (CBC-MAC) AES-CCMP 128-bit keys to ensure the integrity of the data in transmission. AES-CCMP uses authenticated encryption modes, including a counter for confidentiality and CBC for authenticity, with a single key. It also relies on CBC-MAC for authentication, integrity, and replay protection, and provides a 64-bit message integrity check (MIC). The IEEE 802.11i specification provides the most robust Layer 2 security for federal agencies while meeting FIPS 140-2 requirements. It is standards-based and facilitates vendor interoperability.

## Protecting the Network

The final requirement in deploying the WLAN is to ensure the ongoing protection of the network. Steps need to be taken to ensure the protection of not only the WLAN but also the wired network. To address the protection of the WLAN Cisco recommends the deployment of Adaptive wIPS.

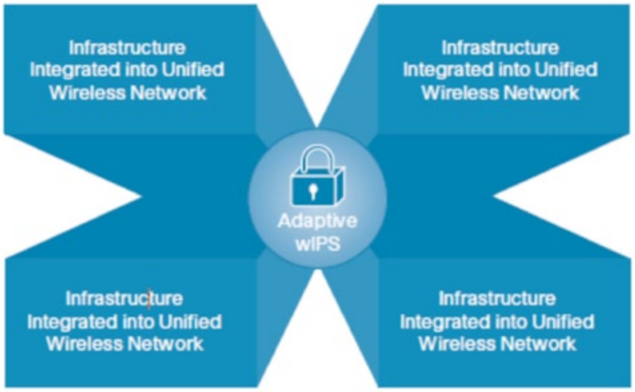
The Cisco infrastructure-integrated approach to detection– combining air monitoring, network traffic, anomaly analysis, real-time network device and topology information, and network configuration analysis– delivers a comprehensive view of the event to the Cisco Adaptive wIPS analysis engine. With that breadth of information, Adaptive wIPS can detect events not traceable with over-the-air signatures alone, and it can make more accurate detection decisions, thus increasing effectiveness while reducing false positives.

The Cisco Adaptive wIPS solution delivers the following key features and benefits:

- Detects and uses customizable rules to auto-classify rogue access points, rogue clients, spoofed clients, and client ad hoc connections. Uses administrator-defined mitigation policies that decrease the time to identify and manage rogue threats
- Protects against over-the-air attack types, including network reconnaissance, authentication and encryption cracking, denial of service, man-in-the-middle, impersonation attempts, and new and unknown attack techniques to provide comprehensive protection throughout the RF environment
- Assesses wireless security vulnerabilities throughout the network by constantly monitoring the security posture of the wireless network in real time to prevent attacks before they can happen
- Provides an extensive attack, vulnerability, and performance detection library, giving wireless administrators the knowledge they need to protect wireless networks without being security experts
- Shields wired and wireless networks against wireless threats to help enable federal customers to meet stringent wireless policies dictating wireless IDS requirements

Figure 6 illustrates how Cisco Adaptive wIPS sits in the heart of the network.

Figure 6. Cisco Adaptive wIPS


Infrastructure Integrated into Unified Wireless Network
Infrastructure Integrated into Unified Wireless Network
Adaptive wIPS
Infrastructure Integrated into Unified Wireless Network
Infrastructure Integrated into Unified Wireless Network

Layer 2 wireless security can not defend the network when a valid authenticated user inadvertently launches a layer 3 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 or disassociates the client device at the edge of the network, extending customers' security control to the perimeter.

The IEEE 802.11w standard provides protected management frames. 802.11w secures the management frame communications between a client and an access point by appending all frames with authenticated, signed AES message integrity code (MIC). 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.

Cisco has long supported a pre-802.11w implementation, called 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 (for example, de-authorization attacks, and others) revert to just degrading performance by contending with valid clients. This encrypts management frames sent between access points and MFP-capable client stations so that both the access point and client can take preventive action by dropping spoofed management frames (such as those passed between an access point 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. As clients emerge that support 802.11w, Cisco will provide full 802.11w support.

## Bring Your Own Device (BYOD)

The U.S. Equal Employment Opportunity Commission (EEOC) was among the first of several federal agencies to implement a BYOD pilot that allowed employees to opt out of the government-provided mobile device program. They could install third-party software on their own smartphones that enabled the use of their device for official work purposes.

Cisco has seen demand for BYOD solutions grow across all business sectors. The Cisco BYOD Smart Solution utilizing the Cisco Unified Wireless Network is a complete BYOD solution that can be easily tailored to meet the needs of government agencies. It includes proven solution designs, professional and technical support services, and network infrastructure and access points so that WLANs can be built and supported with policy-enforced, highly secure access; exceptional network experiences; and simplified operations.

With the Cisco BYOD Smart Solution, access to data, applications, and systems can be secured with a single policy management plane across the organization, including guest, posture, and device profiling; network access; and mobile device management (MDM). Cisco also provides highly secure access to data in the network (on and off premises) to help ensure IP protection.

## Enterprise WLAN for Unclassified Network

The Cisco Unified Wireless Network architecture also meets the security requirements for the Sensitive But Unclassified (SBU) network, a U.S. government designation that, while including unclassified information, still requires strict controls which are defined broadly in the DoD Instruction 8420.01 and the DISA STIG.

SBU networks in the U.S. government include individual tax records held by the Internal Revenue Service and information in these designations:

- For Official Use Only (FOUO)
- Law Enforcement Sensitive (LES)
- Security Sensitive Information (SSI)
- Critical Infrastructure Information (CII)

## Cisco Unified Wireless Network Products for the Federal Market

Cisco delivers a comprehensive portfolio of government-certified networking products, with more than 200 certifications for products that have completed the most rigorous government testing procedures, including FIPS, DoD UC APL, and Common Criteria.

Cisco Unified Wireless Network products include the following:

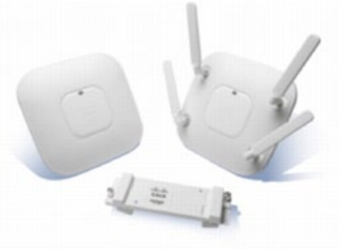
## Cisco Aironet 3600, 3500, 2600, and 1600 Series Access Points

The Cisco Aironet 3600 Series introduces ClientLink 2.0 to boost performance and range for all 802.11n and 802.11a/g devices, including 1, 2, and 3 spatial stream clients. The 3600 Series builds on the Cisco heritage of proactive interference protection with Cisco CleanAir technology. The 3600 Series Access Point is the industry’s first 4x4 MIMO, 3-spatial-stream access point.

Cisco Aironet 3600 Series is an innovative, modular platform that offers superior investment protection with future module expansion to support incoming 802.11ac clients with 870 megabits per second (Mbps) rates or comprehensive security and spectrum monitoring and control. (See what the product looks like in Figure 7.)

Certifications include: FIPS 140-2 Level 2 (in process)

Figure 7. Cisco Aironet 3600 Series Access Points



Cisco Aironet 3500 Series Access Points with Cisco CleanAir technology are the industry's first 802.11n access points to create a self-healing, self-optimizing wireless network. CleanAir technology is a systemwide feature of the Cisco Unified Wireless Network that improves air quality by detecting RF interference that other systems can't recognize, identifying the source, locating it on a map, and then making automatic adjustments to optimize wireless coverage. These innovative access points provide high-performance 802.11n connectivity for mission-critical mobility. By intelligently avoiding interference, the 3500 Series offers performance protection for 802.11n networks to help ensure reliable application delivery. (Product images are provided in Figure 8.)

Certifications include: DoD UC APL, Common Criteria, and FIPS 140-2 Level 2

Figure 8. Cisco Aironet 3500 Series Access Points

The Cisco Aironet 2600 Series Access Point delivers highly advanced features in its class, with superior performance, functionality, and reliability at an affordable price. The 802.11n-based Aironet 2600 Series includes 3x4 MIMO, with three spatial streams, plus Cisco CleanAir, ClientLink 2.0, and VideoStream technologies, to help ensure an interference-free, high-speed wireless application experience. Second to the Cisco Aironet 3600 Series in performance and features, the Aironet 2600 Series sets a new standard for enterprise wireless technology.

Designed with rapidly evolving mobility needs in mind, the Aironet 2600 Series Access Point is packed with more BYOD-enhancing functionality than any other access point at its price point currently offers. It sustains reliable connections at higher speeds farther from the access point than competing solutions, resulting in more availability of 450-Mbps data rates. Optimized for consumer devices, the Aironet 2600 Series accelerates client connections and currently consumes less mobile device battery power than competing solutions.

Certifications include: FIPS 140-2 Level 2 (in process)

The Cisco Aironet 1600 Series Access Point is an enterprise-class, entry-level, 802.11n-based access point designed to address the wireless connectivity needs of small- and medium-sized enterprise networks. The Aironet 1600 Series delivers strong performance at an attractive price for customers. It provides advanced functionality such as CleanAir Express for better coverage through spectrum intelligence, and ClientLink 2.0 for entry-level networks that have a mixed client base. In addition to these features, the Aironet 1600 series includes 802.11n-based 3x3 MIMO technology with two spatial streams, making it ideal for small and medium-sized enterprises.

The Aironet 1600 Series provides at least six times the throughput of existing 802.11a/g networks. As part of the Cisco Aironet Wireless portfolio, the Cisco Aironet 1600 Series Access Point provides low total cost of ownership and investment protection by integrating seamlessly with the existing network. With an entry-level path to 802.11n migration, the Aironet 1600 Series can add capacity to the network for future growth for expanding applications and bandwidth.

Designed with rapidly evolving mobility needs in mind, the Cisco Aironet 1600 Series Access Point addresses the BYOD trend by providing advanced functionality at an attractive price point.

## Cisco 5508 Wireless Controller

The Cisco 5500 Series Wireless Controller (see Figure 9) is a highly scalable and flexible platform that can enable systemwide services for mission-critical wireless in medium- to large-sized enterprises and campus environments. Designed for performance and maximum scalability, the 5500 Series offers enhanced uptime with the ability to simultaneously manage 500 access points and 7000 devices; 8-Gigabit Ethernet (GE) ports with Link Aggregation Groups (LAG) support; superior performance for reliable streaming video and toll quality voice; and improved fault recovery for a consistent mobility experience in the most demanding environments.

Certifications include: FIPS 140-2 Level 2

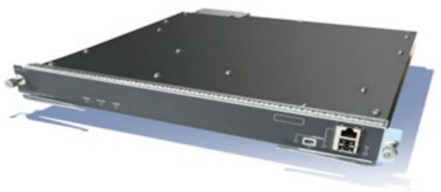
Figure 9. Cisco 5500 Series Wireless Controller

## Cisco Wireless Services Module 2 (WiSM2)

The WiSM2 is a Catalyst 6500 Service Module that is integrated and highly scalable, and extends the same policies and security from the wired network core to the wireless edge. The WiSM2 provides medium-sized to large, single-site WLAN deployments with exceptional performance, security, and scalability to support mission-critical wireless business communications. It helps to lower hardware costs and offers flexible configuration options that can reduce the total cost of operations and ownership for wireless networks. The WiSM2 provides additional scalability over the 5508 Wireless Controller, including connections for up to 1000 access points and 15,000 clients. This provides support for higher client density than other wireless LAN controllers and the ability to update 500 access points at once. (Figure 10 includes a product image of the WiSM2.)

Certifications include: FIPS 140-2 Level 2

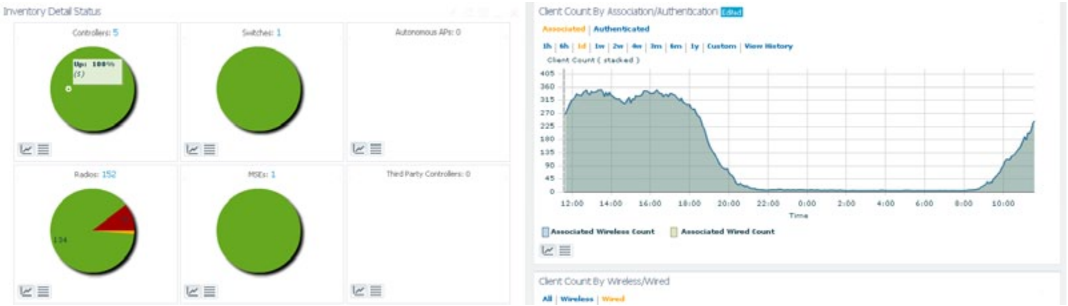
Figure 10. Cisco WiSM2



## Cisco Prime Infrastructure

Part of the Cisco Prime Infrastructure bundle, the Cisco Prime Network Control System (NCS) provides converged user, access, and identity management across wired and wireless networks to meet the challenges that BYOD is placing on IT organizations. Designed with users and their mobile devices in mind, Cisco Prime NCS speeds network troubleshooting by giving IT complete visibility into connectivity, regardless of device, network, or location. Deep integration with the Cisco ISE further extends this visibility across security and policy-related problems, presenting a complete view of client issues with a clear path to solving them. Cisco Prime NCS (Figure 11) delivers full lifecycle management of Cisco WLAN infrastructure, with additional focus on the deployment and management of branch networks.

Figure 11. Cisco NCS



## Cisco Mobility Services Engine (MSE)

The Cisco 3300 Series MSE is a combination of hardware and software infrastructure, providing a practical approach for the delivery of mobility services and applications. The open platform 3355 appliance or virtual machine support a suite of software to provide centralized and scalable delivery of various mobility services. The two key services provided by the MSE are Context Aware and Adaptive wIPS services. The MSE also plays a pivotal role in the delivery of CleanAir capabilities.

Figure 12. Cisco 3300 Series MSE

## Cisco Identity Services Engine (ISE)

The Cisco ISE is a next-generation identity and access control policy platform that can enable enterprises to facilitate new business services, enhance infrastructure security, enforce compliance, and simplify service operations. Its unique architecture allows enterprises to gather real-time contextual information from networks, users, and devices to make proactive governance decisions by enforcing policy across the network infrastructure–wired, wireless, and remote. The Cisco Identity Services Engine is an integral component of the Cisco TrustSec® solution and SecureX Architecture®.

The Cisco ISE provides a single policy plane across the entire organization that combines multiple services, including authentication, authorization, and accounting (AAA), posture, profiling, device on-boarding, and guest management, on a common platform. This reduces complexity and provides consistency across the enterprise. Using the Cisco ISE, administrators can centrally create and manage access control policies for users and endpoints in a consistent fashion and gain end-to-end visibility into everything that is connected to the network.

Certifications include: FIPS 140-2 Level 1.

## 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. Younger workers entering the workforce are accustomed to wireless access and expect to be able to check email, 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 and productivity
- Increased worker satisfaction

## 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 can enable 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.

Cisco provides an industry-leading, 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 can significantly reduce both capital expenditures and operating expenses while it increases a mobile workforce's productivity.

## Increased Collaboration and Productivity

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 email 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 email and receive voice communications without the IT staff having to do prior configurations. 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 54.3 percent of the market share for enterprise WLAN products by Gartner Group in June 2012. 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 non-essential applications to enterprisewide, pervasive networks than run mission- critical applications like wireless voice over (VoIP) and enterprise resource planning. The strength of Cisco Unified Wireless Network solutions lies in the following areas.

## Unified Access Simplified

The Cisco Unified Access (UA) solution provides design guidance on how to solve key business problems related to network access–on-campus or remotely–with traditional devices such as laptops and desktops, as well as non-traditional devices, such as mobile phones and tablets. Unified Access is an integrated solution that brings together security, mobility, management, and intelligent network infrastructure. Unified Access clearly illustrates the importance of network infrastructure as the foundation for intelligently and dynamically solving network access challenges.

The three supporting pillars of the Cisco Unified Access solution are:

- One policy – single source of policy across wired, wireless, and remote access
- One management – manage user experience end to end
- One network – deliver a seamless experience across any network

## 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 (ISRs).

## Industry-Leading Security

As the number of wireless endpoints (laptops, personal digital assistants, smart phones, etc.) 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, Cisco can both better 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 IETF CAPWAP. This means they will integrate easily with existing customer investments. For example, deployments that use the Cisco Catalyst 6500 WiSM take advantage of the powerful security, voice, and high availability capabilities of your existing infrastructure.

Where standards are not yet available, Cisco leads industry-wide 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 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, as proven by the more than 70,000 Cisco customers using WLAN solutions and nearly three million Cisco access points deployed worldwide.

## Conclusion

U.S. federal government agencies are increasingly deploying WLANs to reap many enhanced efficiency and cost benefits. To ensure consistent security and quality standards, agencies such as the DoD have issued guidelines and requirements for WLANs.

The Cisco Unified Wireless Network architecture–including unique technologies such as Cisco Unified Wireless, Cisco CleanAir, Cisco VideoStream, Cisco ClientLink, and Cisco Band Select, and an array of WLAN products– is designed to support industry-leading mobility services. It does so in a state-of-the-art, highly secure environment that can improve the end-user experience as it delivers anytime, anywhere connectivity to employees using multiple types of media. This architecture can meet the most stringent guidelines and requirements of the U.S. federal government, providing highly secure, scalable, flexible, and easily managed WLAN solutions. With extensive global WLAN experience and leadership in the WLAN industry, Cisco is helping to extend the value of existing networks through WLAN solutions that improve employee productivity, enhance customer satisfaction, lower costs, and increase the agility of government organizations.

## For More Information

DISA STIG requirements from Wireless STIG - Version 6, Release 5
http://iase.disa.mil/stigs/net_perimeter/wireless/wireless_net.html

DoD 8100.01
http://www.dtic.mil/whs/directives/corres/pdf/800001p.pdf

77DoD 8420.01
http://www.dtic.mil/whs/directives/corres/pdf/810002p.pdf

NIST Guidelines for Securing WLANs
http://csrc.nist.gov/publications/nistbul/february-2012_itl-bulletin.pdf

NIST Security Profile – Configuration Requirements for FIPS Mode
http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp1447.pdf

Cisco Common Criteria Certified Products
http://www.cisco.com/web/strategy/government/security_certification/net_business_benefit_seccert_common_criteria.html

Cisco FIPS-Certified Products
http://www.cisco.com/web/strategy/government/security_certification/net_business_benefit_seccert_fips140.html

Cisco DoD UC APL-Certified Products
http://www.cisco.com/web/strategy/government/security_certification/net_business_benefit_secvpn_dod.html

Cisco Wireless LAN Controller Configuration Guide
http://www.cisco.com/en/US/partner/docs/wireless/wcs/7.0MR1/configuration/guide/hard.html

Cisco Identity Services Engine
http://www.cisco.com/en/US/products/ps11640/index.html

White Paper: The Policy Governed Network
http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5712/ps11640/white_paper_c11-663616.pdf

## Federal Certifications, Guidelines, and Policies for WLANs

Various federal certifications for WLANs in government agencies are outlined in Table 1.

Table 1. Federal WLAN Certifications Overview

| Certification | Description |
|---|---|
| FIPS | These standards and guidelines were developed by the National Institute of Standards and Technology (NIST) for federal computer systems. Considered a benchmark for security in government, FIPS 140-2 validation assures users that a given technology has passed rigorous testing under either the Cryptographic Algorithm Validation Program (CAVP) or Cryptographic Module Validation Program (CMVP) by an accredited third-party lab and can be used to secure sensitive information. There are multiple FIPS publications, but FIPS 140-2 is the only one with an approved product list. FIPS 140-2 validation is required for sale of all products implementing cryptography to the federal government. |
| Unified Capabilities (UC) Approved Products List (APL) | The DoD UC APL maintains a single consolidated list of products that have completed Interoperability (IO) and Information Assurance (IA) certification. Use of the DoD UC APL allows DoD departments to purchase and operate UC systems over all DoD network infrastructures. The APL is the only listing of equipment by the DoD to be fielded in DoD networks. DoD departments are required to fulfill system needs by purchasing only APL listed products, provided that one of the listed products meets department needs. For most DoD customers, this means the APL must be consulted prior to purchasing a system or product. |
| Unified Capabilities Requirements (UCR) | The UCR 2008 specifies technical standards for telecommunication switching equipment to be connected to the Defense Information System Network (DISN), with an emphasis on Military Unique Features, (for example, Multilevel Precedence and Preemption [MLPP]). The UCR specifies requirements for WLAN Access Systems (WLAS) and Wireless Access Bridges (WABs). The UCR Change 2, released in January 2011, added the requirement that the system must use Configuration and Provisioning of Wireless Access Points (CAPWAP). |
| Joint Interoperability Test Command (JITC) | Listing on the DoD UC APL satisfies DoD Instruction 8420.01, which requires JITC evaluation. JITC conducts testing of national security systems and information technology systems hardware, software, and components. JITC testing requirements are based on DoD policy, Defense Information Systems Agency (DISA) Network Infrastructure Security Technical Implementation Guides (STIGs), and the UCR requirements. |
| DoD Information Assurance Certification and Accreditation Process (DIACAP) | The DIACAP is the U.S. DoD process to ensure that risk management is applied on information systems. DIACAP defines a DoD-wide standard set of activities, general tasks, and a management structure process for the certification and accreditation of a DoD information system that will maintain the Information Assurance posture throughout the system's life cycle. |
| DISA STIGs | The DISA STIG defines what an organization must do to satisfy the standards of DoD IA and IA-enabled devices and systems. Wireless standards are defined by the Wireless STIG - Version 6, Release 5. Key configuration requirements for WLANs include:<br>• WLAN must be WPA2-enterprise approved by the Wi-Fi Alliance<br>• Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) authentication using the DoD CAC is required to ensure EAP-TLS is FIPS validated<br>• Transmitted data must use FIPS-validated 802.11i using Advanced Encryption Standard Counter Cipher Mode with Block Chaining Message Authentication Code Protocol (AES-CCMP) encryption and must be WPA2-enterprise certified<br>• The site will conduct continuous wireless intrusion detection system (IDS) scanning; this requirement applies to all DoD sites that operate DoD computer networks, including sites that have no authorized WLAN systems<br>• In-band management traffic must be FIPS-validated<br>• Wireless access points and bridges must be placed in dedicated subnets outside the enclave’s perimeter<br>The Cisco Unified Wireless Network can be configured to meet all of these requirements. |
| Common Criteria | Another relevant WLAN standard that many federal agencies utilize. It is an international standard for evaluating IT product security and reliability. It is recognized by more than 26 countries around the world, including Australia, Canada, France, Germany, Greece, Italy, Japan, New Zealand, Spain, the United Kingdom, South Korea, and the United States. Many government customers around the world consider Common Criteria a mandatory requirement for purchasing network security products, and these standards in other countries are relevant to U.S. Common Criteria standards and vice versa. |

## Guidelines and policies for WLANs in federal government agencies

- DoD Instruction 8100.2, entitled “Use of Commercial Wireless Devices, Services and Technologies in the Department of Defense (DoD) Global Information Grid (GIG).” This document mandates the use of strong authentication, nonrepudiation, and personal identification in accordance with DoD public key infrastructure (PKI). It also states that encryption of wireless traffic using an assured channel is mandatory and must be FIPS140-2-validated. Finally, it mandates wireless intrusion detection, denial of service mitigation, and active screening for wireless devices.

  In June 2006 the DoD issued a second document as supplementary guidance to DoD 8100.2. This document mandates 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).
- DoD instruction 8420.01, issued in November 2009, consolidated the mandates from other directives to provide clear, concise requirements for WLAN deployments in the DoD.

  NIST and the National Security Agency (NSA) have established a program under the National Information Assurance Partnership (NIAP) that is responsible for Common Criteria standards in the U.S. NIAP’s mission is to evaluate IT product conformance to international standards. The program, officially known as the NIAP Common Criteria Evaluation and Validation Scheme for IT Security (CCEVS) is a partnership between the public and private sectors. NIAP-approved Protection Profiles are being created for technologies of high priority for U.S. consumers and the Commercial Solutions for Classified Program. The two WLAN Protection Profiles include: “Protection Profile for Wireless Local Area Network (WLAN) Access Systems – 15 November, 2011, Version 1.0” and “Protection Profile for Wireless Local Area Network (WLAN) Clients – 19 December, 2011, Version 3.1.”
- The Information Technology Laboratory (ITL) of the NIST issued a 2012 list of “Guidelines for Securing WLANs.” Recommendations included employing standard security configurations for common WLAN components, such as client devices and access points; consideration of both the security of the WLAN and how the security of other networks may be affected by the WLAN when developing plans for WLAN security; and implementation of policies that clearly state which forms of dual connections are permitted or prohibited for WLAN client devices and how to enforce these policies through the application of appropriate security controls. The guidelines also recommend that an organization’s WLAN client devices and access points have configurations that are compliant with the organization’s WLAN policies, and that both attack monitoring and vulnerability monitoring be performed along with regular periodic technical security assessments of the organization’s WLANs.

**Americas Headquarters**
Cisco Systems, Inc.
San Jose, CA

**Asia Pacific Headquarters**
Cisco Systems (USA) Pte. Ltd.
Singapore

**Europe Headquarters**
Cisco Systems International BV Amsterdam,
The Netherlands

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.**