Cisco Unified Wireless Security

This chapter describes the natively available 802.11 security options and the advanced security features in the Cisco Unified Wireless solution, and how these can be combined to create an optimal WLAN solution.

The Cisco Unified Wireless solution can also be integrated with other Cisco Security solutions; this integration is covered in Chapter 9, "Cisco Unified Wireless Security Integration."

Overview

As network administrators begin to deploy WLANs, they are faced with the challenge of trying to secure these environments while providing maximum flexibility for their users. The Cisco Unified WLAN architecture has multiple components depending on the implementation, but there are two core components that are common in every solution. These are the LWAPP APs -single and dual radio, shown in Figure 4-1, and the Wireless LAN controller (WLC) shown in Figure 4-2.

Figure 4-1 LWAPP APs

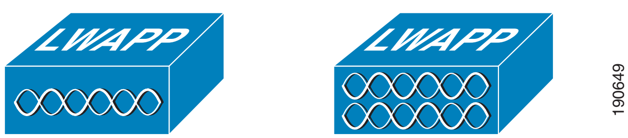
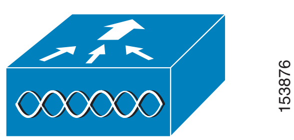


Figure 4-2 LWAPP Controller



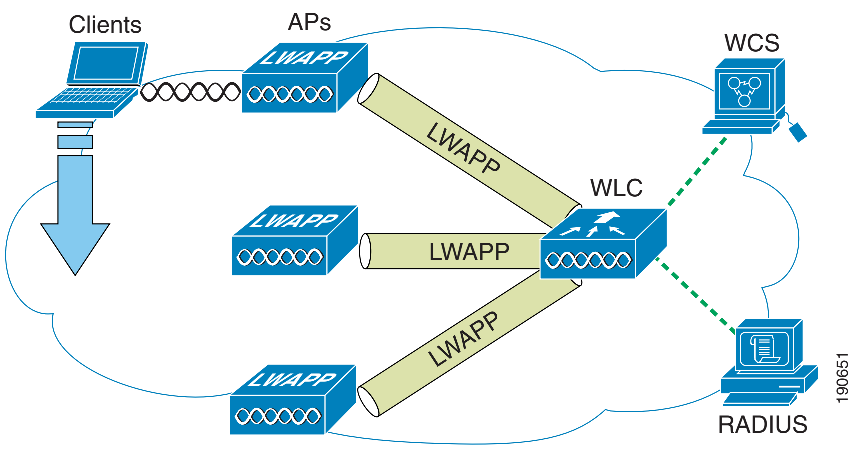
There are various LWAPP AP models and WLC types, but the core WLAN security features remain the same, as does the architecture.

Architecture

The general Cisco Unified WLAN architecture is shown in Figure 4-3, and this architecture can be classified into the following four main layers:

- Client
- Access
- Control and distribution
- Management

Figure 4-3 Unified Wireless Architecture



Functional Areas and Components

This section describes the functional areas and components of the Cisco Unified Wireless solution.

Client Component

The client component is critical to the overall security strategy of the solution because the security capabilities of the client often dictate the security capabilities of the solution.

The client device can be a handheld device such as a scanner, PDA, or VoWLAN handset; a mobile device such as a Table PC or laptop computer; or a fixed device such as a PC or printer.

The Cisco Unified Wireless solution is compatible with standard WLAN clients and many specialized WLAN devices. One of the simplest ways to determine which client works best with the Cisco Unified Wireless solution is to consult the Cisco Certified Extensions (CCX) program to verify which WLAN clients are certified for operation with the Cisco solution, in addition to any advanced features included in CCX. For more information on CCX, see the following URL: http://www.cisco.com/web/partners/pr46/pr147/partners_pgm_concept_home.html.

Access Layer

The Access Layer component is the LWAPP APs, which provide the 802.11a/b/g connection for the client devices, and tunnel the client traffic to and from the LWAPP controller across the enterprise network.

Control and Distribution

The Control and Distribution Layer component is primarily performed by the LWAPP controller, which terminates LWAPP tunnels from the LWAPP APs and directs traffic to the appropriate interface and VLAN. The LWAPP controller is also the administrative and authorization interface for APs, and WLAN clients. The LWAPP controller performs additional roles, such as RF management, wireless IDS, and collects location information.

Authentication

A key component in enterprise WLAN deployments is EAP authentication through a RADIUS server. Authentication services for the Cisco Unified Wireless solution can be provided by the Cisco ACS server, which supports all common EAP types including Cisco LEAP, EAP-FAST, EAP-TLS, and PEAP (MSCHAP and GTC), and provides interfaces into external authentication databases such as Microsoft Active Directory, Novell NDS, LDAP, and RSA token servers. The ACS server can also be configured to proxy to other RADIUS servers.

Management

The LWAPP controller has a comprehensive management interface, but centralized management for the Cisco Unified Wireless solution is provided by the Wireless Control System (WCS). In addition to traditional system management functions, WCS provides RF planning and visualization tools, and location services. WCS is covered in more detail later in this document.

WLAN Security Implementation Criteria

For the WLAN network, security is based on both authentication and encryption. Common security mechanisms for WLAN networks are as follows:

- Open Authentication, no encryption
- Wired Equivalent Privacy (WEP)
- Cisco WEP Extensions (CKIP +CMIC)
- Wi-Fi Protected Access (WPA)
- Wi-Fi Protected Access 2 (WPA 2)

WPA and WPA 2 are defined by the Wi-Fi Alliance, which is the global Wi-Fi organization that created the Wi-Fi brand. The Wi-Fi Alliance certifies inter-operability of IEEE 802.11 products and promotes them as the global, wireless LAN standard across all market segments. The Wi-Fi Alliance has instituted a test suite that defines how member products are tested to certify that they are interoperable with other Wi-Fi Certified products.

The original 802.11 security mechanism, WEP, was a static encryption method used for securing wireless networks. Although it applies some level of security, WEP is viewed as insufficient for securing business communications. In short, the WEP standard within 802.11 did not address the issue of how to manage encryption keys. The encryption mechanism itself was found to be flawed, in that a WEP key could be derived simply by monitoring client traffic. Cisco WLAN products addressed these issues by introducing 802.1x authentication and dynamic key generation and by introducing enhancements to WEP encryption: CKIP and CMIC. 802.11i is a standard introduced by the IEEE to address the security shortcomings of the original 802.11 standard. The time between the original 802.11 standard and the ratification of 802.11i saw the introduction of interim solutions.

WPA is an 802.11i-based security solution from the Wi-Fi Alliance that addresses the vulnerabilities of WEP. WPA uses Temporal Key Integrity Protocol (TKIP) for encryption and dynamic encryption key generation by using either a pre-shared key, or RADIUS/802.1x-based authentication. The mechanisms introduced into WPA were designed to address the weakness of the WEP solution without requiring hardware upgrades. WPA2 is the next generation of Wi-Fi security and is also based on the 802.11i standard. It is the approved Wi-Fi Alliance interoperable implementation of the ratified IEEE 802.11i standard. WPA 2 offers two classes of certification: Enterprise and Personal. Enterprise requires support for RADIUS/802.1x-based authentication and pre-shared key (Personal) only requires a common key shared by the client and the AP. The new AES encryption mechanism introduced in WPA2 generally requires a hardware upgrade from earlier versions of WLAN clients and APs, however all Cisco LWAPP APs support WPA2.

Table 4-1 summarizes the various specifications.

Table 4-1 WLAN Security Mechanisms

Feature	Static WEP	802.1x WEP	WPA	WPA 2 (Enterprise)
Identity	User, machine or WLAN card	User or machine	User or machine	User or machine
Authentication	Shared key	EAP	EAP or pre-shared keys	EAP or pre-shared keys
Integrity	32-bit Integrity Check Value (ICV)	32-bit ICV	64-bit Message Integrity Code (MIC)	CRT/CBC-MAC (Counter mode Cipher Block Chaining Auth Code - CCM)
Encryption	Static keys	Session keys	Per Packet Key rotation via TKIP	CCMP (AES)
Key distribution	One time, Manual	Segment of PMK	Derived from PMK	Derived from PMK
Initialization vector	Plain text, 24-bits	Plain text, 24-bits	Extended IV-65-bits with selection/sequencing	48-bit Packet Number (PN)
Algorithm	RC4	RC4	RC4	AES
Key strength	64/128-bit	64/128-bit	128-bit	128-bit
Supporting infrastructure	None	RADIUS	RADIUS	RADIUS

The Cisco Wireless Security suite provides the user with the options to provide varying security approaches based on the required or pre-existing authentication, privacy and client infrastructure. Cisco Wireless Security Suite supports WPA and WPA2, including:

- Authentication based on 802.1X using the following EAP methods:
  - Cisco LEAP, EAP-Flexible Authentication via Secure Tunneling (EAP-FAST)

- PEAP- Generic Token Card (PEAP-GTC)
- PEAP-Microsoft Challenge Authentication Protocol Version 2 (PEAP-MSCHAPv2)
- EAP-Transport Layer Security (EAP-TLS)
- EAP-Subscriber Identity Module (EAP-SIM)

- Encryption:
  - AES-CCMP encryption (WPA2)
  - TKIP encryption enhancements: key hashing (per-packet keying), message integrity check (MIC) and broadcast key rotation via WPA TKIP Cisco Key Integrity Protocol (CKIP) and Cisco Message Integrity Check (CMIC)
  - Support for static and dynamic IEEE 802.11 WEP keys of 40 bits, 104, and 128 bits

Note 128 bit WEP (128 bit WEP key =152 bit total key size as IV is added to key) is not supported by all APs and clients. Even if it was, increasing WEP key length does address the inherit security weaknesses of WEP.

IPsec

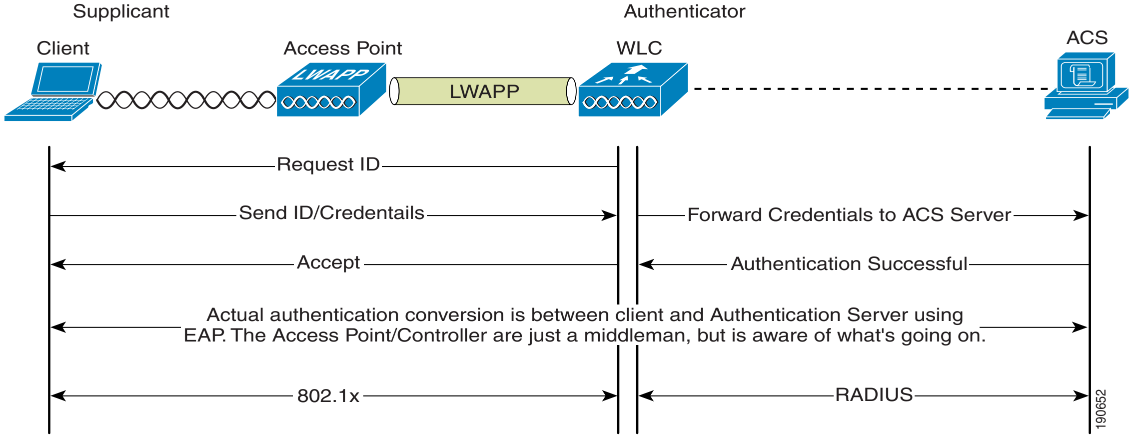
In addition to the variety of security mechanism supported natively in 802.11, authentication and encryption can also be performed at higher network layers. The most common mechanism being IPsec, which is typically implemented in place of or in addition to 802.11 security mechanisms.

The operation of IPsec is not covered in this chapter; however, where appropriate, IPsec-related features and design recommendations for WLAN deployments are made.

802.1x/EAP Authentication

802.11i specifies the use of 802.1x for providing port access control on WLAN network ports. WPA, and WPA2 further specify the use Extensible Authentication Protocol (EAP) to exchange authentication information. EAP payloads are placed within 802.1x frames or RADIUS packets to establish communication between the supplicant -WLAN client, and the Authenticator = AP/WLC -RADIUS server. Access to the network is determined by the success or failure of the EAP authentication, and the WLAN encryption is derived from shared cryptographic data created during the EAP authentication. Figure 4-4 shows the general authentication flow.

Figure 4-4 Generic EAP over 802.1x Authentication Mode



Various EAP types are used in WLAN solutions. Some common EAP types are the following:

- EAP-TLS (transport layer security-PKI-based client and server authentication)
- Cisco Lightweight Extensible Authentication Protocol (LEAP)
- Protected Extensible Authentication Protocol (PEAP)
- Flexible Authentication via Secured Tunnel (EAP-FAST)

These EAP types define how the authentication messaging takes place between the client and the authentication server. The Supplicant and the Authentication Server must support the same EAP types. Because the EAP payloads are passed across the Authenticator without being parsed, the Authenticator need not care about the EAP authentication type. EAP payload data of interest to the Authenticator comes from a successful authentication. Such data might include RADIUS VSAs specifying the VLAN ID to be used by the client, ACLs, or controlling QoS parameters.

Although the Authenticator need not know the EAP type used, Authenticator configuration can impact the successful implementation of a given EAP type; for example, the 802.1x timeouts and retries parameters can impact the usability of PEAP-GTC because it requires a user to enter data.

Table 4-2 provides a brief comparison of various EAP supplicants.

Table 4-2 EAP Authentication Comparison

	Cisco LEAP	Cisco EAP-FAST	PEAP/MS-CHAPv2	PEAP(EAP-GTC)	EAP-TLS
Single sign-on (MSFT AD only)	Yes	Yes	Yes	Yes[1]	Yes
Login scripts execution (MSFT AD only)	Yes	Yes	Yes	Some	Yes[2]
Password Change (MSFT AD)	No	Yes	Yes	Yes	N/A
Cisco 350 and CB20A client support for Windows XP, 2000, and Windows CE OS	Yes	Yes	Yes	Yes	Yes
PCI card client support for Windows XP and Windows 2000	Yes	Yes	Yes	Yes	Yes
Microsoft AD DB support	Yes	Yes	Yes	Yes	Yes
ACS local DB support	Yes	Yes	Yes	Yes	Yes
LDAP DB support	No	Yes[3]	No	Yes	Yes
OTP authentication support	No	Yes [8]	No	Yes	No

Table 4-2 EAP Authentication Comparison (continued)

RADIUS server certificate required?	No	No	Yes	Yes	Yes
Client certificate required?	No	No	No	No	Yes
Susceptible to Dictionary attacks?	Yes[4]	No	No	No	No
Susceptible to MITM attacks?	No	No[5]	Yes[6]	Yes[7]	No
Fast secure roaming (Cisco CCKM)	Yes	Yes	Yes[1]	Yes[1]	Yes[1]
Local authentication	Yes	Yes	No	No	No
WPA support (Windows 2K/XP)	Yes	Yes	Yes	Yes	Yes
Proactive Key Caching (PKC WPA2 802.11i Fast Roaming)	Yes	Yes	Yes	Yes	Yes

[1] Supplicant Dependent

[2] Machine account on Windows AD is required to enable Login Script execution for PEAP and EAP-TLS

[3] Automatic provisioning is not supported for LDAP back-end DBs. Manual provisioning would have to be used for back-end LDAP DBs.

[4] Strong Password policy is required for LEAP deployment to mitigate risks because of offline (such as passive) dictionary attacks.

[5] EAP-FAST with automatic provisioning is susceptible to rogue server (reduced MITM) attack during the phase 0 (automatic provisioning stage). MITM attacks require the attacker to spoof a legitimate AP. Which means strategies such as Rogue AP detection and Management Frame Protection can detect the presence of these attacks.

[6] PEAP (specifically PEAPv1) is vulnerable to MITM attacks.

This MITM vulnerability will be fixed in PEAPv2.

[7] Although Cisco PEAP, as a hybrid authentication type, is theoretically vulnerable to MITM attacks, the Cisco supplicant implementation of PEAPGTC is less vulnerable, as it does not accept the same authentication types inside and outside the TLS tunnel, a requirement for the MiTM exploit publicly detailed. OTP Authentication supported in EAP-FAST v1a.

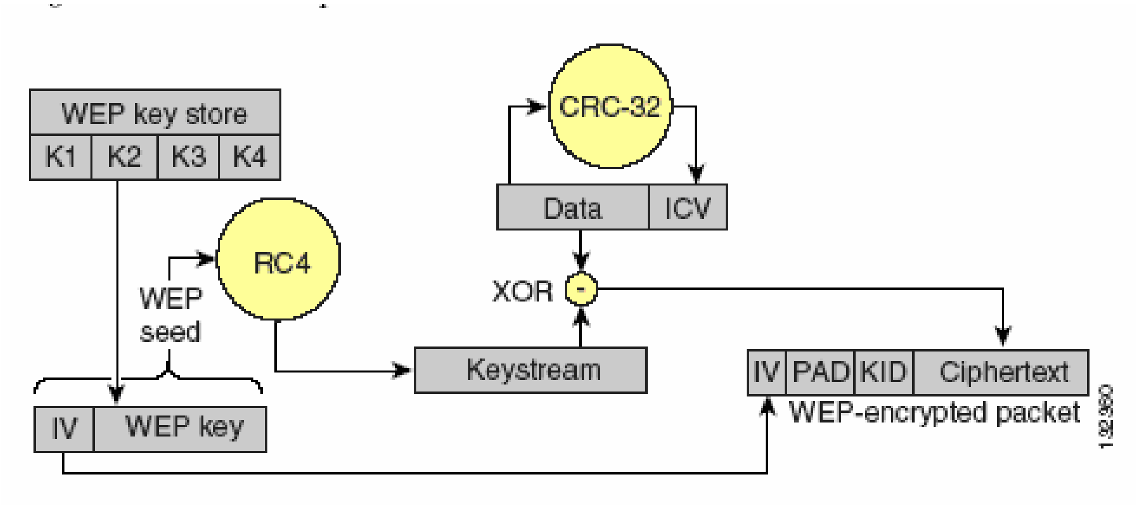
[8] For comment on EAP-FAST OTP support Supplicant Dependent

Wired Equivalent Privacy

This section provides a brief description of encryption and message integrity mechanisms (see Figure 4-5). The main goals for encryption and message integrity are to prevent disclosure, modification, and insertion of packets in a WLAN.

References to sources that provide more detailed information and an analysis of crypto-algorithms, key management, and implementations can be found in References, page 4-12.

Figure 4-5 WEP Encapsulation Process



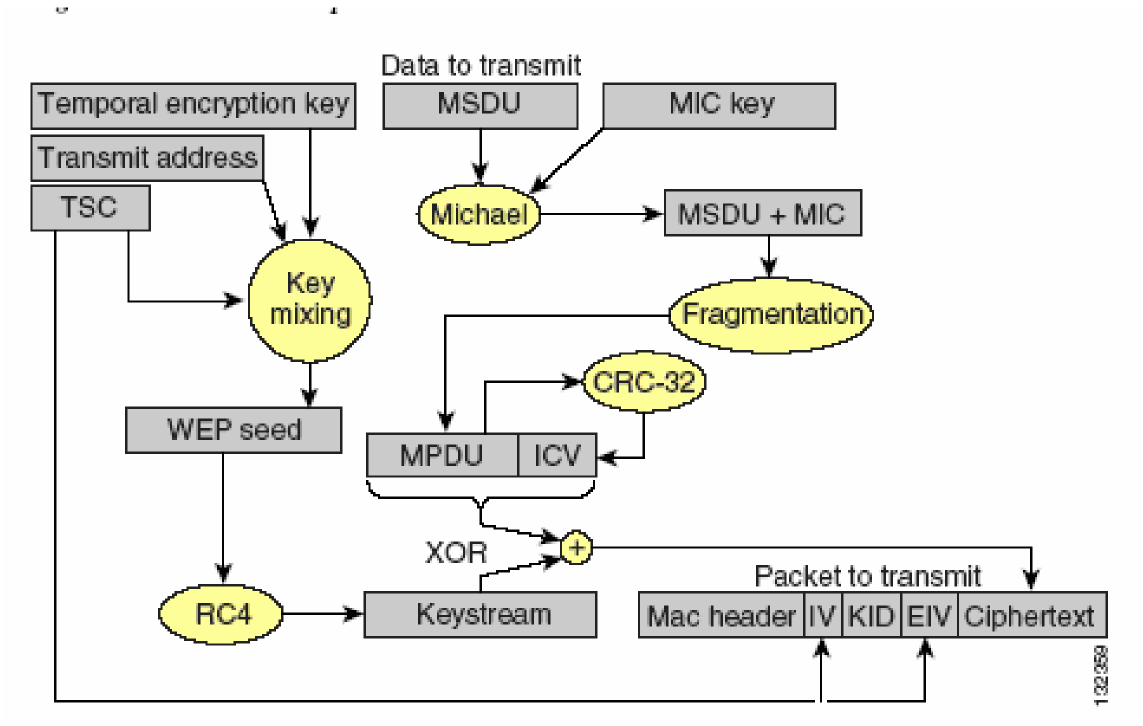
The LWAPP WLAN solution supports three key lengths: the standard 40 and 104 bit key lengths, and an additional 128 bit key. The use of the 128 bit key is not recommended because 128 bit keys are not widely supported in WLAN clients, and the additional key length does not address the weakness inherent in WEP encryption

Temporal Key Integrity Protocol

With TKIP, the main objective is to address the problems with WEP and to work with legacy hardware; therefore, the base encryption mechanism is still RC4, the same as WEP.

TKIP is a cipher suite that includes key mixing algorithms and a packet counter to protect the keys. It also includes the Michael Message Integrity Check (MIC) algorithm that, along with the packet counter, can prevent packet modification and insertion. Figure 4-6 illustrates the TKIP encapsulation process.

Figure 4-6 TKIP Encapsulation Process



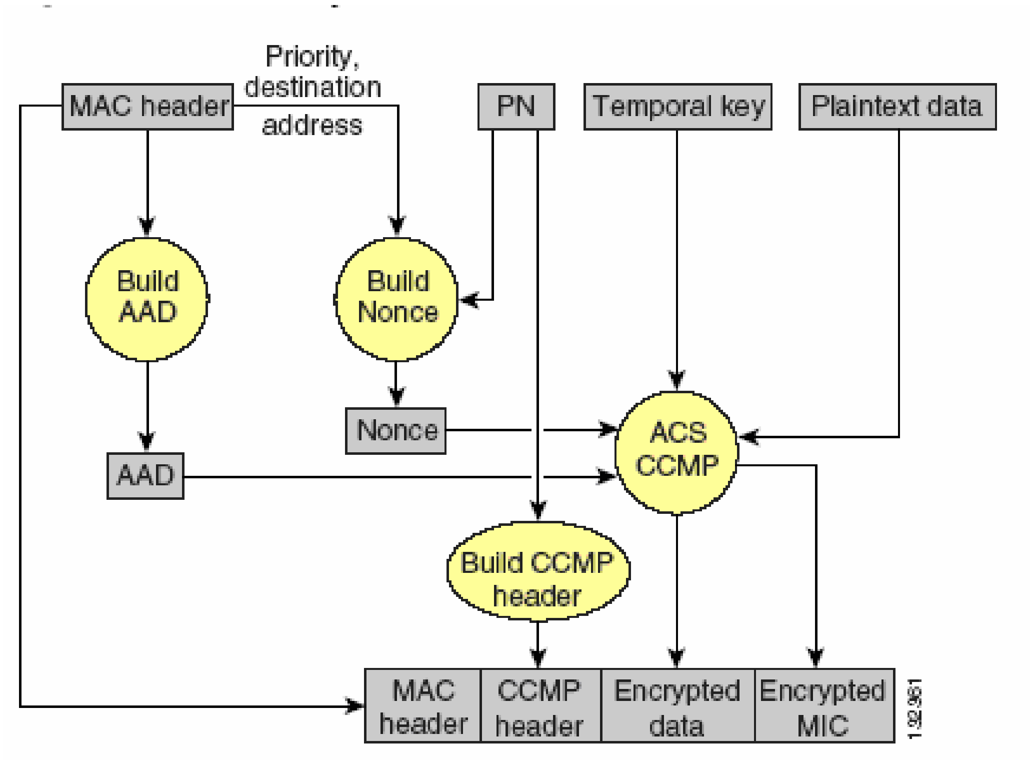
Cisco Key Integrity Protocol and Cisco Message Integrity Check

Cisco Key Integrity Protocol (CKIP) and Cisco Message Integrity Check (CMIC) are the Cisco versions of TKIP and MIC, respectively. CKIP and CMIC were developed to address the WEP vulnerabilities before the release of WPA. Combined, CKIP and CMIC provide encryption and message integrity far superior to WEP.

Counter Mode/CBC-MAC Protocol

Counter Mode/CBC-MAC Protocol (CCMP) is an algorithm based on the Advanced Encryption Standard (AES). It provides encryption and data integrity, and is part of the 802.11i specification. AES has stronger encryption and message integrity than TKIP, but is not compatible with legacy WLAN hardware because of the much more intensive processing required for AES encryption and decryption. Figure 4-7 illustrates the CCMP encapsulation process.

Figure 4-7 CCMP Encapsulation Process

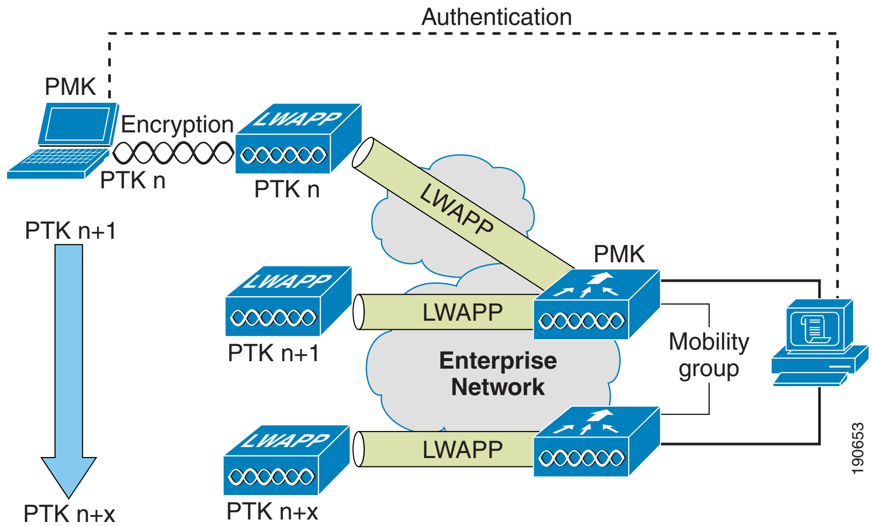


Proactive Key Caching and CCKM

Proactive Key Caching (PKC) is an 802.11i extension that allows for the proactive caching (before the client roaming event) of the Pair-wise Master Key (PMK) that is derived during a client 802.1 x/EAP authentication at the AP (see Figure 4-8). If a PMK (for a given WLAN client) is already present at an AP when presented by the associating client, full 802.1x/EAP authentication is not required. Instead, the WLAN client can simply use the WPA four-way handshake process to securely derive a new session encryption key for communication with that AP.

The distribution of these cached PMKs to APs is greatly simplified in the Unified Wireless deployment. The PMK is simply cached in the controller(s) and made available to all APs that connect to that controller, and between all controllers that belong to the mobility group of that controller in advance of a client roaming event.

Figure 4-8 Proactive Key Caching Architecture



Cisco Centralized Key Management (CCKM) is a Cisco standard supported by CCX clients to provide Fast Secure Roaming. The principle mechanism for accelerating roaming is the same as PKC, by using a cached PMK, but the implementation is slightly different and the two mechanisms are not compatible.

The state of the each WLAN client's key caching can be seen with the **show pmk-cache all** command This identifies which clients are caching the keys, and which key caching mechanism is being used.

The 802.11r workgroup is responsible for the standardization of a fast secure roaming mechanism for 802.11. The WLC controller supports both CCKM and PKC on the same WLAN -802.1x+CCKM, as shown in the following example:

```
WLAN Identifier.................................. 1
Network Name (SSID).............................. wpa2
…
Security
   802.11 Authentication:........................ Open System
   Static WEP Keys............................... Disabled
   802.1X........................................ Disabled
   Wi-Fi Protected Access (WPA/WPA2)............. Enabled
      WPA (SSN IE)............................... Disabled
      WPA2 (RSN IE).............................. Enabled
         TKIP Cipher............................. Disabled
         AES Cipher.............................. Enabled
   Auth Key Management
         802.1x.................................. Enabled
         PSK..................................... Disabled
         CCKM.................................... Enabled
…
(Cisco Controller) >show pmk-cache all
PMK-CCKM Cache
                            Entry
Type        Station          Lifetime   VLAN Override       IP Override
------    --------------    --------   ------------------   ---------------
CCKM     00:12:f0:7c:a3:47   43150                            0.0.0.0
RSN     00:13:ce:89:da:8f   42000                            0.0.0.0
```

References

There are many articles and books that cover security in detail, such as the following:

- *Cisco Wireless LAN Security* by Sankar, Sundaralingam, Balinsky and Miller
- *802.11 Real Security* by Edney and Arbaugh
- *802.11 Wireless Fundamentals* by Roshan and Leary

WLAN Security Selection

There are many options for selecting and implementing the security standards for WLANs. However, in most implementations, the decisions are bound by existing enterprise security practices and clients participating in the WLANs, When dealing with clients, you need to know what supplicants are available for those clients, and specifically what authentication/identity framework is used by the enterprise.

Given these options, the decision of what must be implemented can be varied and challenging. Cisco provides the ability to segment various security schemes via VLANs, which is described in a separate white paper.

The following tables compare and summarize the security standards for WLANs. Table 4-3 compares Cisco LEAP, PEAP, and EAP-TLS.

Table 4-3 Comparing LEAP, PEAP, EAP-TLS

Cisco LEAP	Supports many operating systems (Windows 95, 98, 2000, XP, Me, NT, Mac OS, Linux, DOS, Windows CE)
	Supports many adapters and client devices, including devices with small processors
	Supports a variety of wireless LAN devices like Cisco workgroup bridges, wireless bridges, and repeaters
	Does not require certificates or a Certificate Authority
	Can be configured quickly and easily
	Supports a single sign-on with an existing user name and password
	Has been field-proven since 2001
	Requires minimal client software overhead
	Utilizes minimal authentication messaging
	Known security exposure—requires strong passwords
EAP-FAST	Tunnel establishment is based on shared secret keys that are unique to users. (Protected Access Credentials (PACs) and can be distributed automatically (Automatic or In-band Provisioning) or manually (Manual or Out-of-band Provisioning) to client devices.)
	Single sign-on (SSO) using the user name and password supplied for Windows networking logon
	Wi-Fi Protected Access (WPA) support without third-party supplicant (Windows 2000 and XP only)
	Support for key Cisco Unified WLAN Architecture features: Fast Secure Roaming (CCKM) and Local

Table 4-3 Comparing LEAP, PEAP, EAP-TLS (continued)

	RADIUS Authentication
	No reliance on Microsoft 802.1X framework
	No certificates authority needed/ No requirement for certificates
	Windows Password Aging (support for server-based password expiration)
EAP-TLS	Supported natively on Windows XP and Windows 2000 (with service pack)
	Supports NDS and LDAP (when appropriately configured)
	Uses same PKI mechanism as wired or dial-up access for easy distribution of client certificates
	Official EAP type tested with Wi-Fi Protected Access (WPA)– although other EAP types will work with WPA
	Exposes user information in the certificate
PEAP-MSCHAP	Supports password change at expiration
	Is defined in a draft RFC
	Does not expose the logon user name in the EAP Identity Response
	Is not vulnerable to a dictionary attack
	Requires a server certificate and CA certificate, but does not require per-user certificates
	The authentication protocol is protected by a TLS tunnel but the tunneled authentication protocol is limited to MSCHAPv2
	Supported natively on Windows XP and Windows 2000(with service packs),
	Integrates into Active Directory user database
PEAP-MSCHAPv2	Support for key Cisco Unified WLAN Architecture features: Fast Secure Roaming (CCKM) and Local
	RADIUS Authentication
	No reliance on Microsoft 802.1X framework
	No certificates authority needed/ No requirement for certificates
PEAP-GTC	Supports authentication using one-time passwords
	Supports NDS and LDAP
	Supports password change at expiration
	Is defined in a draft RFC
	Does not expose the logon user name in the EAP identity response
	Is not vulnerable to a dictionary attack
	Requires a server certificate and CA certificate, but does not require per-user certificates

Table 4-4 lists the advantages of using 802.1x EAP for WLAN.

Table 4-4 802.1x Comparison to IPsec VPN

802.1x EAP Types versus IPsecVPNs	The advantages of using 802.1X EAP for WLAN are:·
	Included with Wi-Fi certified clients and access points
	Minimal client software overhead
	Minimal authentication messaging overhead
	Minimal management overhead
	Natively supported on many operating systems
	Layer 3 roaming support
	Authentication choice for enterprise deployments

Table 4-5 compares the advantages of Cisco TKIP with WPA TKIP.

Table 4-5 Cisco KIP Comparison to WPA TKIP

Cisco TKIP	WPA TKIP
Cisco TKIP is well-suited to the following deployments: • Enhanced security is required but a WPA supplicant cannot be supported on the client platform. • If 802.1q trunks are supported by the Layer 2 infrastructure and it is possible to use WLAN VLANs to segregate Cisco TKIP users from other WLAN users.	WPA TKIP is well suited to the following deployments: • Client devices can support WPA. • Cisco Compatible version 2 cards in use. • If 802.1q trunks are not supported by the Layer 2 infrastructure WPA and non-WPA clients can operate on the same SSID, via WPA migration mode. Native support for wireless devices and authentication protocol is desired (no external supplicant required).

Table 4-6 lists the advantages and disadvantages of using VPN for WLAN.

Table 4-6 Advantages and Disadvantages of Using VPN for WLAN

Advantages	Disadvantages
Uses 3DES or AES encryption	Client software overhead
Enforces remote user authentication and polices for Wireless LAN users	Authentication messaging overhead
Leverages existing VPN if already installed for wired network	Management overhead because one VPN application is required per client
Used for remote users accessing the network while on the road at airports, hotels, conference centers	Does not support single sign on using Windows log-in

Table 4-6 Advantages and Disadvantages of Using VPN for WLAN (continued)

	Client traffic is hidden from WLAN infrastructure, limiting the application of any policies based on client traffic
	Limited or no multicast and multiprotocol support

WLAN Security Configuration

The WLC allows the configuration of multiple WLANs that can be mapped to different dot1q interfaces on the WLC, and the WLANs can applied to different APs through AP grouping.

Figure 4-9 shows the main configuration page for WLAN security on WLC. This is part of the WLAN menu; each WLAN that is created has a similar page where key 802.11 parameters can be configured, as well as the security settings for that WLAN. These security settings include the type of authentication and encryption to be used for that WLAN, including any sub-options applicable to that security option. For example, solutions that require 802.1x based authentication allow RADIUS servers to be selected for that authentication type.

Figure 4-9 WLAN Configuration Page

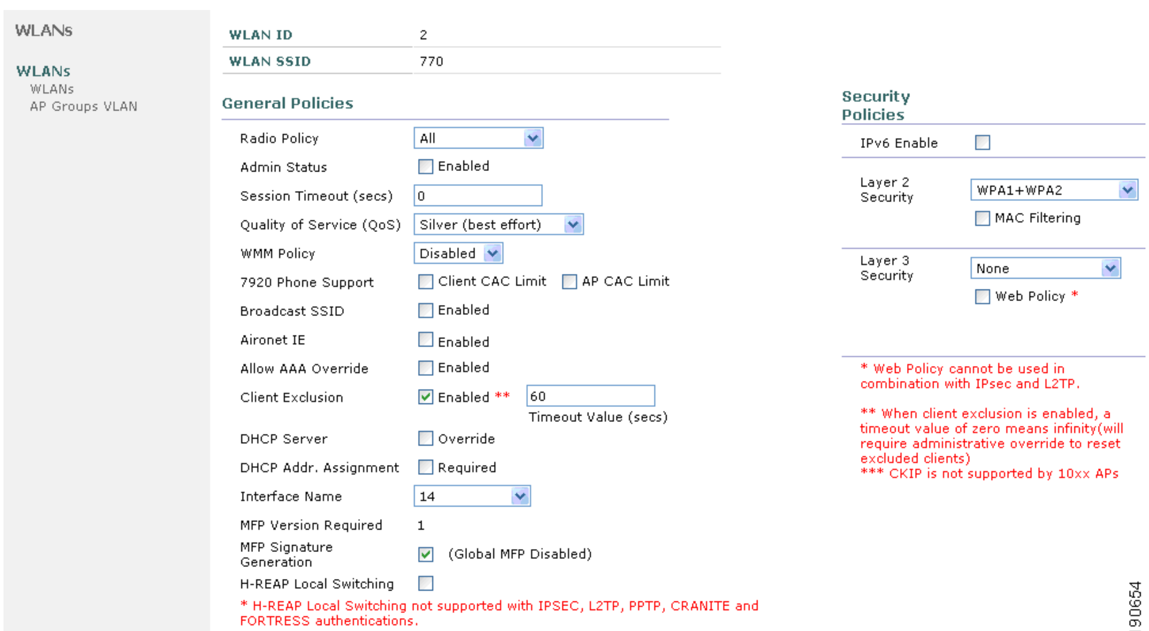
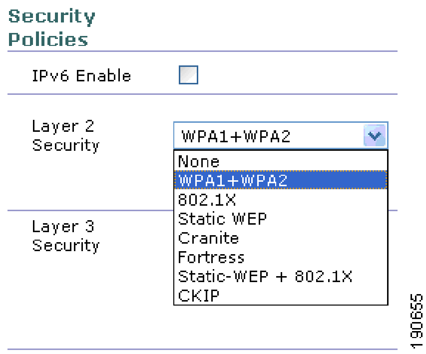


Figure 4-10 shows the various Layer 2 security options that are available on the WLAN. These range from Open Authentication with no encryption to WPA-2.

Figure 4-10 Controller WLAN Layer 2 Security Options



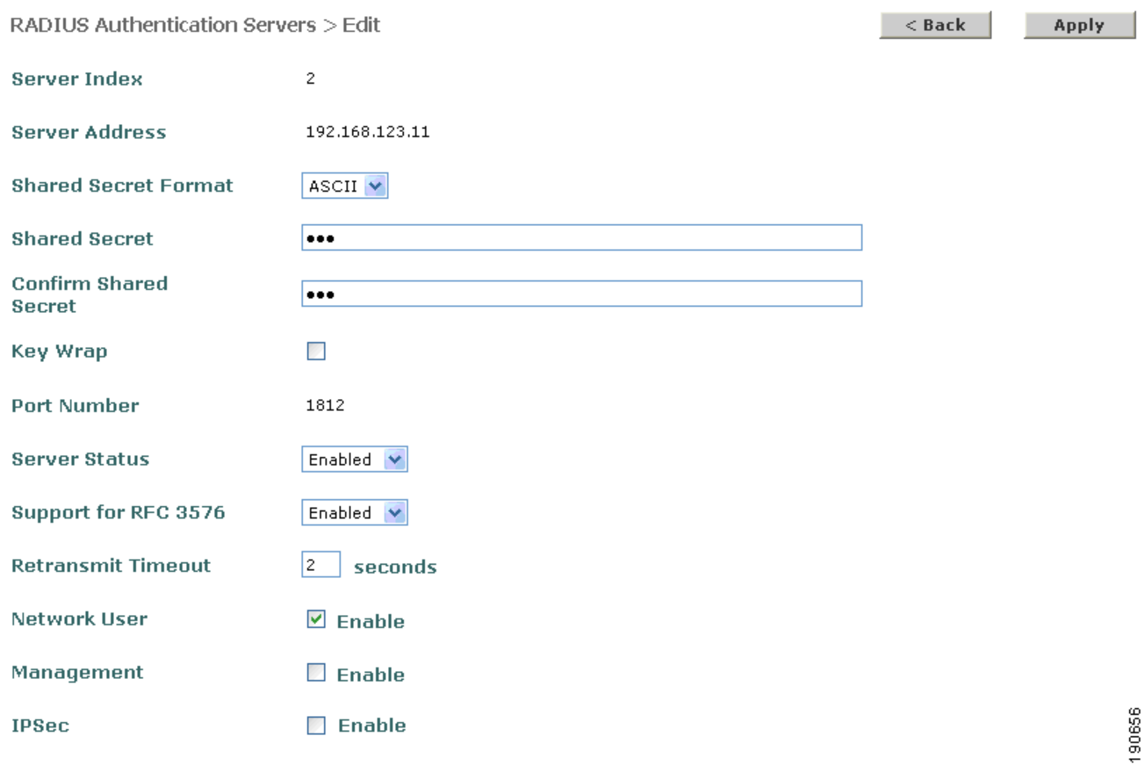
The RADIUS servers used in the WLAN configuration are configured on the controller in the security section, shown in Figure 4-11. Multiple RADIUS servers can be configured, and assigned different priorities. Note that the RADIUS server priority setting from Figure 4-11 is not the priority of the RADIUS servers used in the WLAN authentication, that priority is established on the WLAN configuration page.

The Retransmission timeout sets the delay between retransmission if the RADIUS server does not respond to the RADIUS request. The WLC retries five times before trying the next RADIUS server in a configured list.

Note that the WLC does not automatically retry the preferred RADIUS server when it has failed over to another server, unless that server stops responding; for example, the RADIUS server does not fail back.

Note also that the source address used by the controller for AAA authentication is the management address of the WLC.

Figure 4-11 RADIUS Configuration



The Key WRAP option should be left unchecked unless a RADIUS server using the Key WRAP features (typically in a FIPS compliant implementation) is being configured.

Unified Wireless Security

The Cisco Unified WLAN Architecture addresses many facets of WLAN security, and although this white paper focuses on WLAN Data Transport Security, a brief description of the other security features of the solution is described in this section. The security features are grouped into the following three categories:

- Infrastructure Security—Security features addressing the configuration and deployment of the WLAN solution itself
- WLAN Data Transport Security—The security features addressing the WLAN traffic
- WLAN Environment Security—The security features designed to protect the WLAN environment and resources from attack or accidental interference

Infrastructure Security

The deployment of WLANs in enterprises generally involves the deployment of enterprise network equipment in locations other than locked wiring closets, or Network Operating Centers (NOC). This introduces a new exposure to some networks, because it increases the likelihood of the theft or attacks on network equipment, which can in turn expose authentication keys, encryption keys, passwords, and other configuration data relating to network security.

The Cisco Unified WLAN Architecture is immune to the vulnerabilities described above by virtue of the fact that the centralized architecture does not store any security configuration information in NVRAM within the LWAPP APs themselves (configuration is lost when power is removed from the AP). Instead, all configurations related to WLAN and system security are implemented in the LWAPP controller, which is typically deployed in a secured location. The privacy of network configuration is further enhanced by its encryption between the LWAPP AP and the LWAPP controller, and by preventing console access to the LWAPP AP configuration. This prevent the WLAN configuration information being learned through capturing the LWAPP stream of reading the configuration on an active AP.

The Cisco Unified WLAN Architecture also prevents the threat of impersonation and spoofing to gain access to network configuration information through the use of X.509 certificates on the LWAPP devices, and also requires PKI authentication before LWAPP configuration information is exchanged. In addition, the MAC addresses contained in the X.509 certificates can be authenticated against a centralized database(s) to ensure that unauthorized APs do not connect to a controller.

The WLC, which is the core component of the Cisco Unified WLAN solution, uses dot1q VLANs to provide isolation between user WLAN traffic, and the WLC's management interfaces. The WLC also offers secure management access using SSH, HTTPS, and SNMPv3 protocols, as well as providing an out of band management interface on many WLC models.

Additionally, the WLC allows ACLs to be implemented to further restrict access. This is accomplished by using the **config acl cpu** command. Applying ACLs directly to the Management and AP-Management WLC interfaces currently has no effect on traffic to the WLC, and only applies to WLAN client traffic on those interfaces. Therefore, when using ACLs to control traffic to the WLC management interfaces, use the **config acl cpu** command.

WLAN Data Transport Security

The Cisco Unified WLAN Architecture provides a full range of WLAN transport security features ranging from open unauthenticated connections to WPA2 connections. These various security models can be supported over the same infrastructure, and mapped to different wired network connections through configuration policies supplied by the controller or from a AAA server.

The Cisco Unified WLAN Architecture also resolves the architectural challenge of segmenting WLAN traffic from wired data traffic by using LWAPP tunnels to transport WLAN user and control data between APs and the controller and then uses other LWAPP controller features such as 802.1q VLANs and or EoIP tunnels to provide further segmentation.

WLAN Environment Security

The Cisco Unified WLAN Architecture users RF Security features to detect and avoid 802.11 interference and control unwanted RF propagation. The WLAN Intrusion Prevention and Location features not only detect rogue devices or potential WLAN threats, but also locates these devices. This enables system administrators to quickly assess the threat level and take immediate action to mitigate threats as required.

A key component that facilitates WLAN Environment Security reporting is the WCS server. WCS collects and correlates information from the WLCs, and links this information with preconfigured location information stored in the WCS.

The WCS is described in more detail in a subsequent chapter.

Rogue AP

A standard AP looks for rogue activity by going off channel for 50 ms to listen for rogue APs, clients, monitor for noise, and channel interference. The channels to be scanned are configured in the global WLAN network parameters for 802.11a and 802.11b/g. Any detected rogue clients or APs are sent to the controller, which gathers the following:

- Rogue AP MAC address
- Rogue AP name
- Rogue connected clients' MAC address
- Whether the frames are protected with WPA or WEP
- The preamble
- SNR
- RSSI

The WLC waits to label this as a rogue client or rogue AP because it might not have been reported by another AP until it completes another scanning cycle (the WLC ensures that its AP and client database are up to date before labeling a client or AP as rogue). The same AP again moves to the same channel to monitor for rogues access points/clients, noise and interference. If the same clients and/or access points are detected, they are listed as a rogue on the controller again. The WLC now begins to determine whether this rogue is attached to the local network or simply a neighboring AP. In either case, an AP that is not part of the managed local WLAN is considered a rogue.

If an AP is configured for "monitor mode", it does not carry user traffic but spends all its time scanning different channels.

If an AP is configured as a rogue detector, its radio is turned off and its role is to listen for MAC addresses, detected by the controller as being rogue APs. The rogue detector listens for ARP packets, and to be effective should be connected to all broadcast domains via trunk link if desired to maximize the likelihood of detection; the AP is still connected to the network via the native VLAN, but monitors other VLANs for ARP frames.

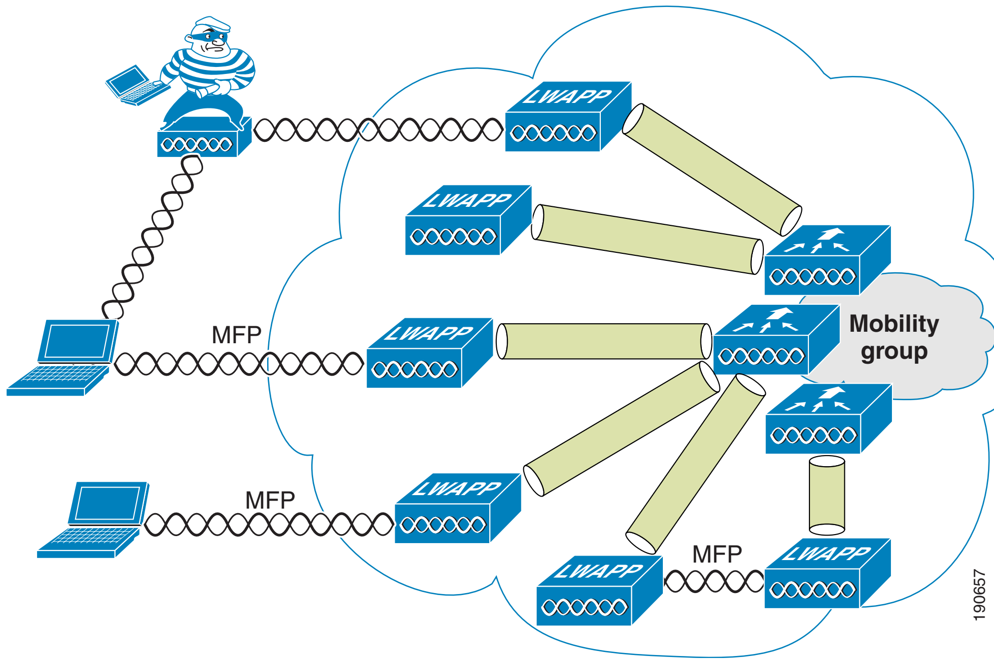
Rogue detector APs might not be practical for some deployments, and do not discover clients that are going through a WLAN router, which are common consumer devices. Rogue Location Discovery Protocol can aid in these cases, where a standard AP, on detecting a rogue AP, can attempt to associate with the rogue AP as a client and send a test packet to the controller. This confirms that the rogue AP is actually on the network The IP addressing information obtained from the test packet can be used to determine the location of the rogue on the network.

Management Frame Protection

One of the challenges in 802.11 has been that management frames are sent unprotected, and are therefore vulnerable to spoofing attacks. To address this, Cisco has created a digital signature mechanism to insert a Message Integrity Check into the 802.11 management frames (see Figure 4-12). This allows legitimate members of a WLAN deployment to be identified, and facilitates easy detection of rogue infrastructure devices through the absence of valid MICs in their management frames.

The message integrity check that is used in MFP is not a simple CRC hashing of the message, but also includes a digital signature component. The MIC component of MFP ensures that a frame has not been tampered with, and the digital signature component ensures that the MIC can have only been produced by a valid member of the WLAN domain. The digital signature key used in MFP is shared among all controllers in a mobility group; different mobility groups have different keys. This allows the validation of all WLAN management frames processed by the WLCs in that mobility group.

Figure 4-12 Management Frame Protection



Currently, MFP is only possible for WLAN infrastructure, but with CCX v5, WLAN clients will be able to learn the mobility group MFP key, and therefore detect and reject invalid frames.

Management Frame Protection provides the following benefits:

- Provides for the authentication of 802.11 management frames by the WLAN network infrastructure
- Allows detection of malicious rogues that are spoofing a valid AP MAC or SSID to avoid detection as a rogue AP, or as part of a man-in-the-middle attack
- Increases the quality of rogue AP and WLAN IDS signature detection
- Will provide protection of client devices with CCX v5
- Also supported with Autonomous AP/ WDS/ WLSE in version 12.3(8)/ v2.13

There are two steps to enable MFP; one to enable it on the WLC, and the second to enable it on the WLAN that is part of the mobility group. Figure 4-13 shows the enabling of MFP on the WLC.

Figure 4-13 Enabling MFP on the Controller

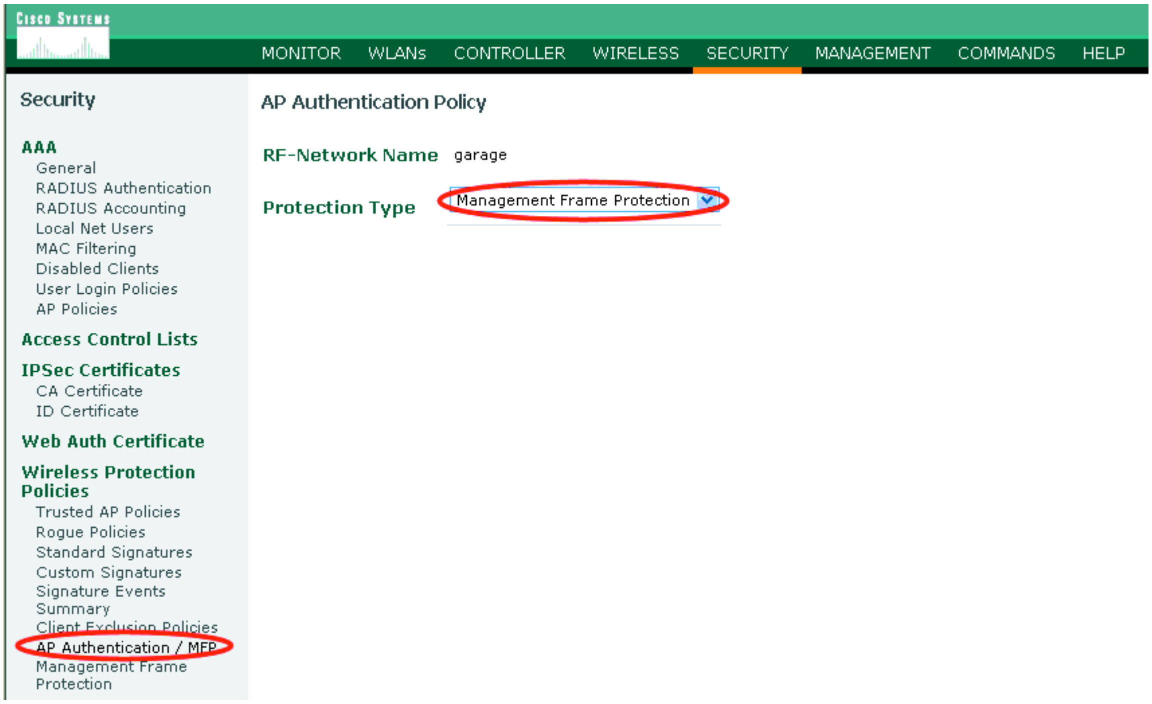
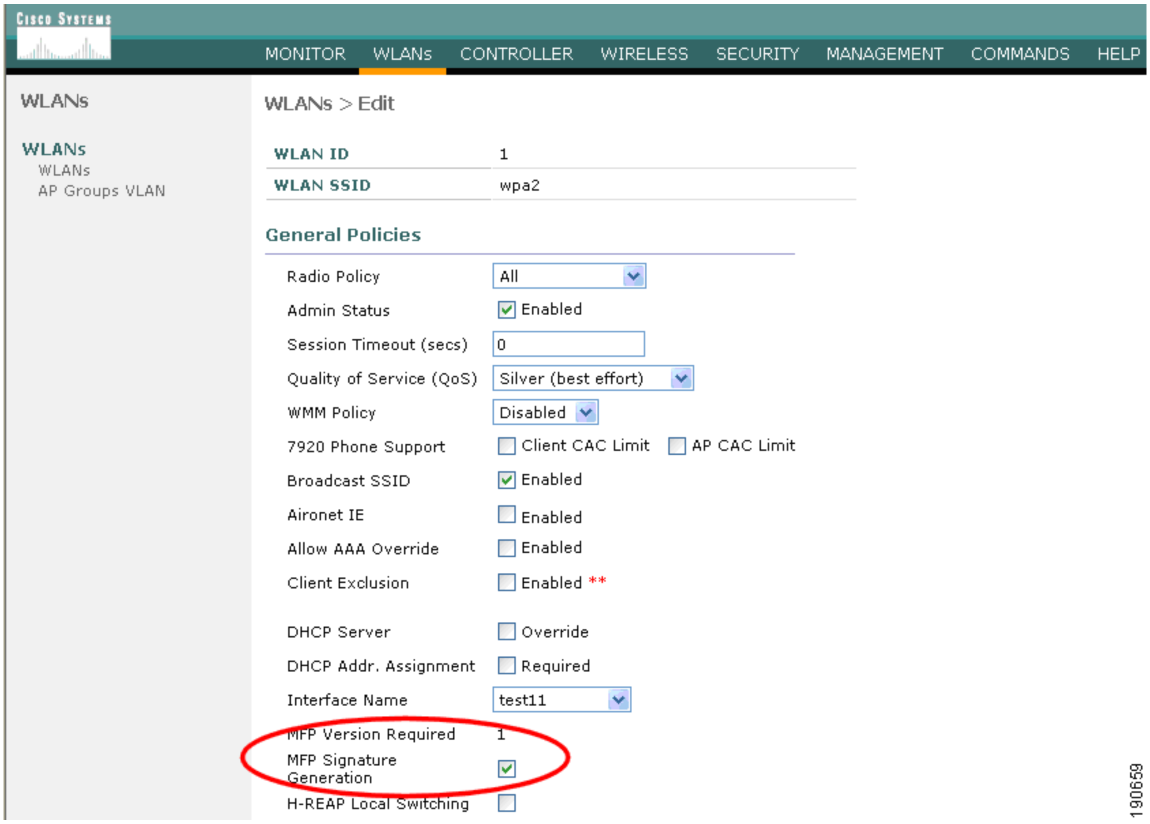


Figure 4-14 shows the enabling of MFP on the WLAN.

Figure 4-14 Enabling MFP per WLAN



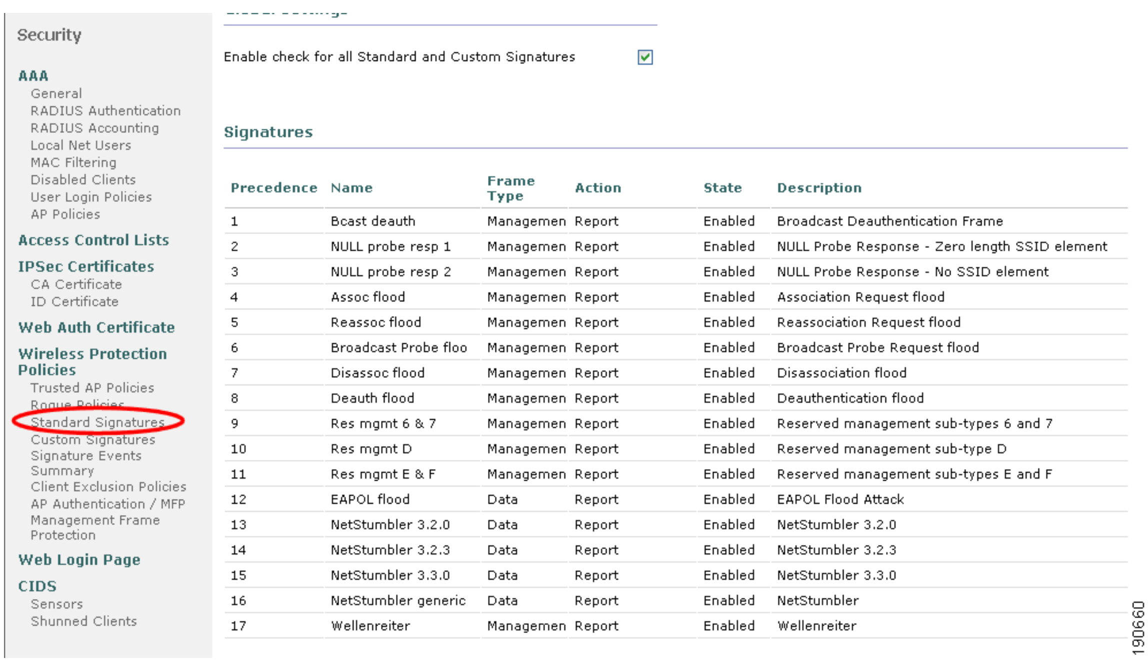
WLAN IDS

The WLC performs WLAN IDS analysis on all its connected WLANs APs, and reports detected attacks at the WLC as well to the WCS. This analysis is separate from the analysis that can be performed by a standalone network IDS system; it analyses 802.11 and WLC specific information that is not otherwise available to a network IDS.

The signature files used on the WLC are included in software releases, but can be updated independently through a signature file; these updated signatures are displayed in the Custom Signatures page.

Figure 4-15 shows the Standards Signatures page on the WLC.

Figure 4-15 Standard WLAN IDS Signatures



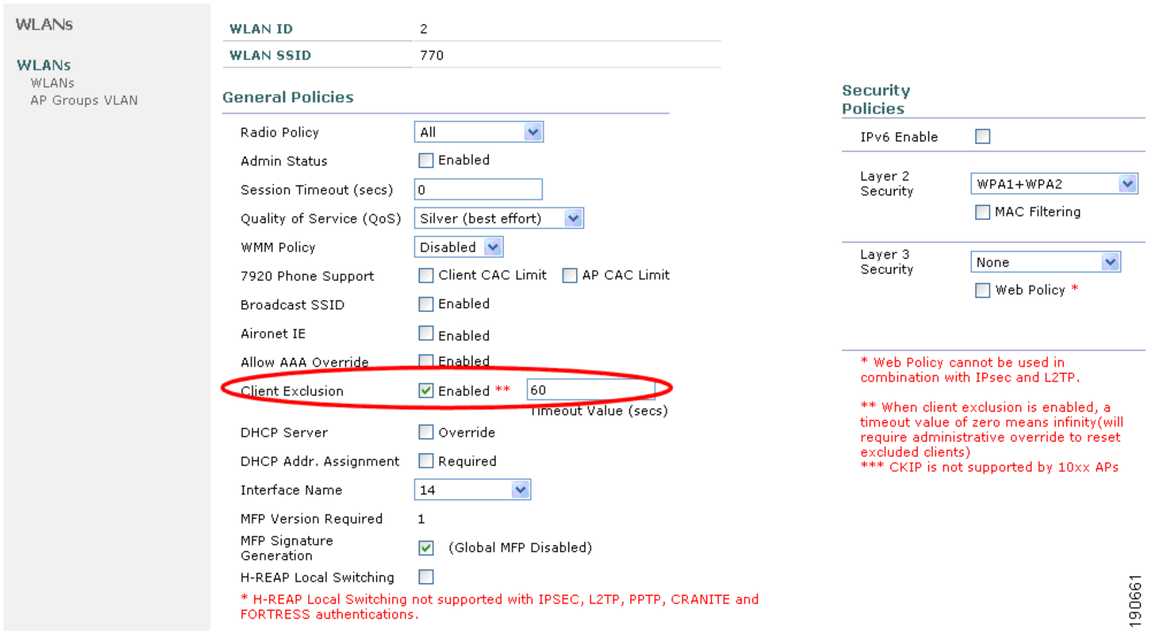
Precedence	Name	Frame Type	Action	State	Description
1	Bcast deauth	Managemen	Report	Enabled	Broadcast Deauthentication Frame
2	NULL probe resp 1	Managemen	Report	Enabled	NULL Probe Response - Zero length SSID element
3	NULL probe resp 2	Managemen	Report	Enabled	NULL Probe Response - No SSID element
4	Assoc flood	Managemen	Report	Enabled	Association Request flood
5	Reassoc flood	Managemen	Report	Enabled	Reassociation Request flood
6	Broadcast Probe floo	Managemen	Report	Enabled	Broadcast Probe Request flood
7	Disassoc flood	Managemen	Report	Enabled	Disassociation flood
8	Deauth flood	Managemen	Report	Enabled	Deauthentication flood
9	Res mgmt 6 & 7	Managemen	Report	Enabled	Reserved management sub-types 6 and 7
10	Res mgmt D	Managemen	Report	Enabled	Reserved management sub-type D
11	Res mgmt E & F	Managemen	Report	Enabled	Reserved management sub-types E and F
12	EAPOL flood	Data	Report	Enabled	EAPOL Flood Attack
13	NetStumbler 3.2.0	Data	Report	Enabled	NetStumbler 3.2.0
14	NetStumbler 3.2.3	Data	Report	Enabled	NetStumbler 3.2.3
15	NetStumbler 3.3.0	Data	Report	Enabled	NetStumbler 3.3.0
16	NetStumbler generic	Data	Report	Enabled	NetStumbler
17	Wellenreiter	Managemen	Report	Enabled	Wellenreiter

Client Security

The IDS features on the WLC provides alarm notifications for possible attacks on the WLAN network. Many of these are initiated by WLAN devices that are connected or attempting to connect to the WLAN network, and these cannot be blocked, only alarmed.

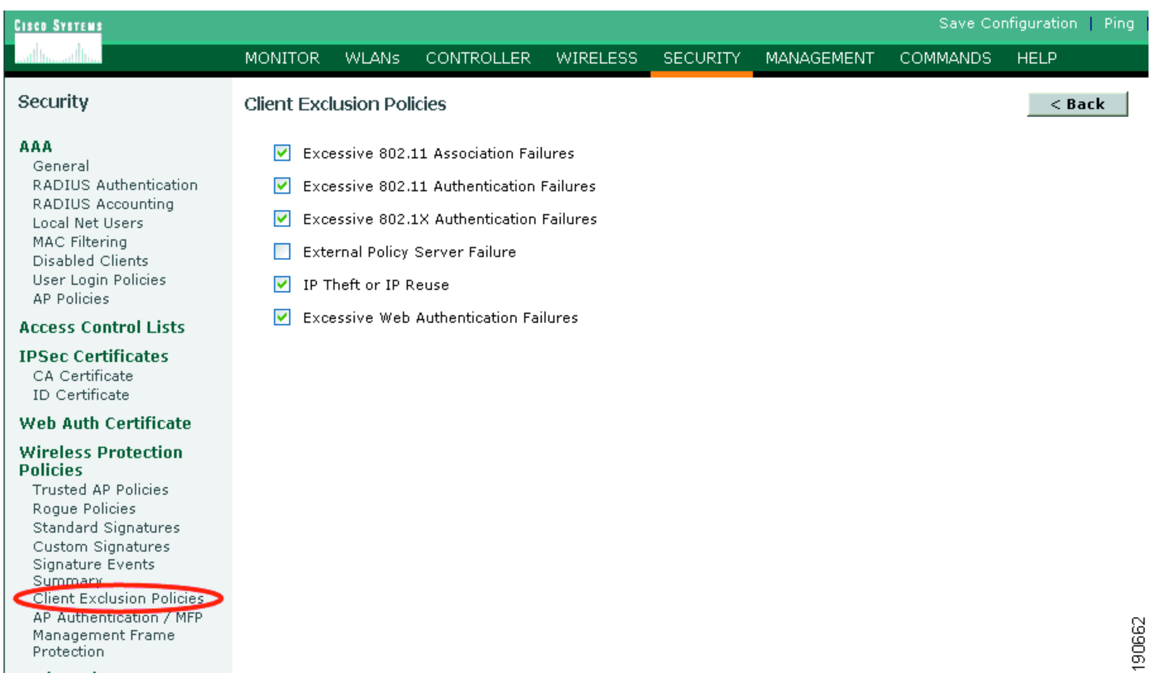
A separate set of client behaviors can be blocked, in addition to some behaviors that might warrant the disconnection of a client from WLAN network altogether. The blocking of clients is controlled through the client exclusion policy. Client exclusion is controlled on a per WLAN basis, as shown in Figure 4-16.

Figure 4-16 Enabling Client Exclusion



The suspect behaviors that cause client exclusion are configured on a per-controller basis, as shown in Figure 4-17.

Figure 4-17 Client Exclusion Policies



WLC Configuration

The three primary methods for configuring the WLC are HTTP, CLI, and SNMP. Each of these has security options. SNMP is covered later in the WCS chapter, but the primary means of securing the user interface is through the PKI encryption of HTTPS, and SSH. Figure 4-18 and Figure 4-19 show the configuration options for HTTP access and CLI access to the WLC. In each case, the encrypted or unencrypted communication mechanism can be selected.

Figure 4-18 HTTP Access to the WLC

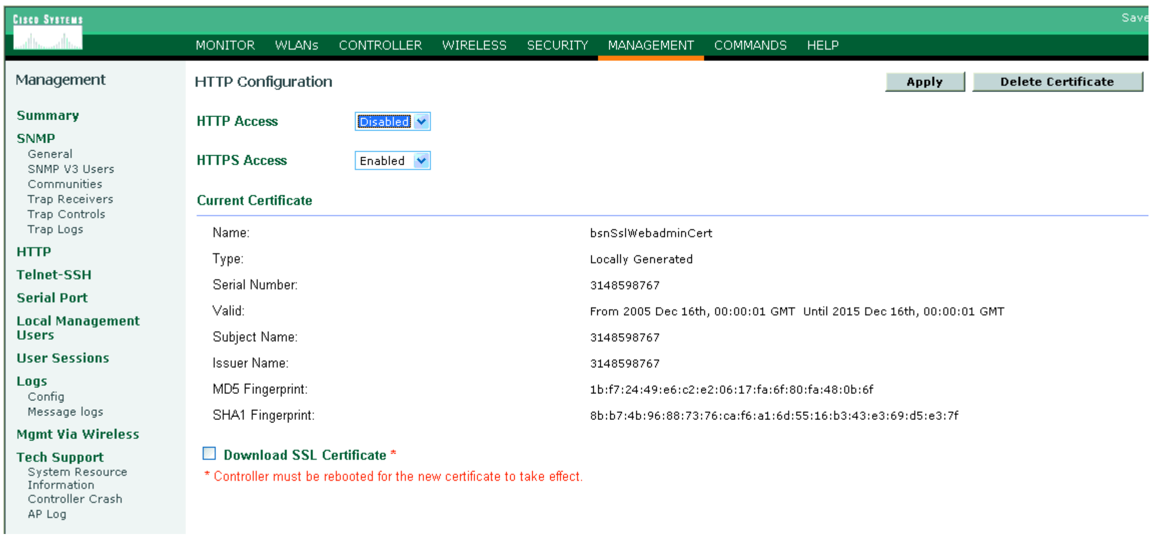
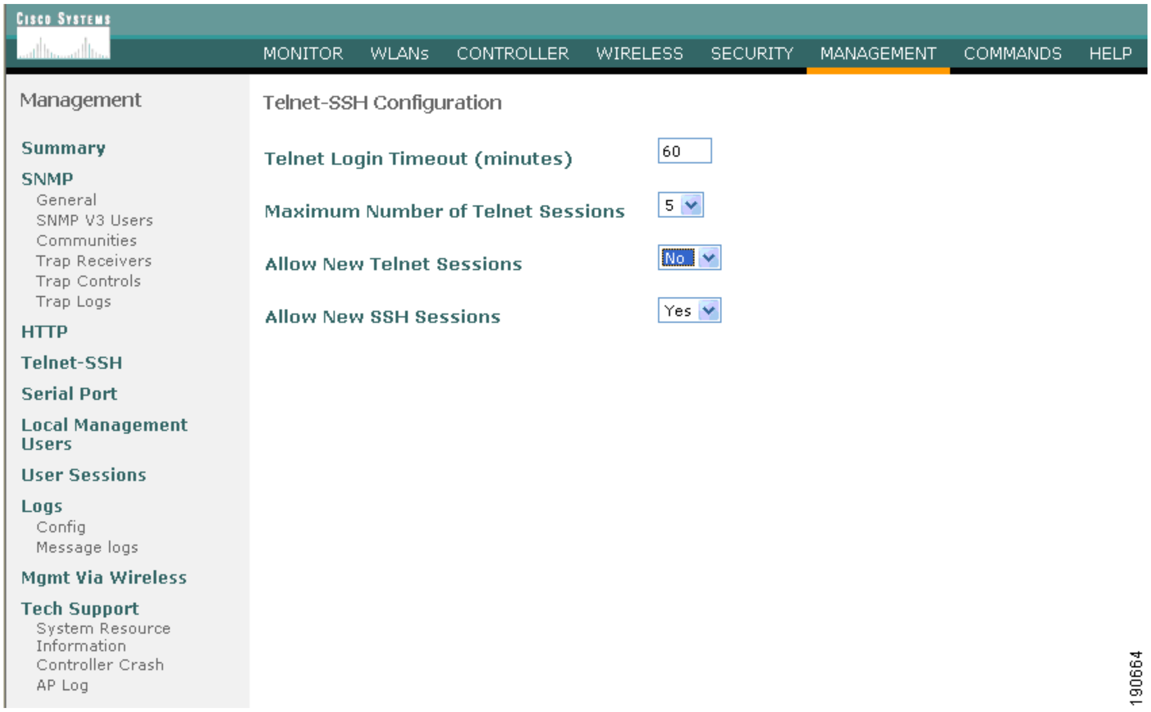


Figure 4-19 CLI Access to the WLC



Management user authentication can be accomplished either through a local database or through a RADIUS server, as shown in Figure 4-20 and Figure 4-21.

Figure 4-20 Local Management Users

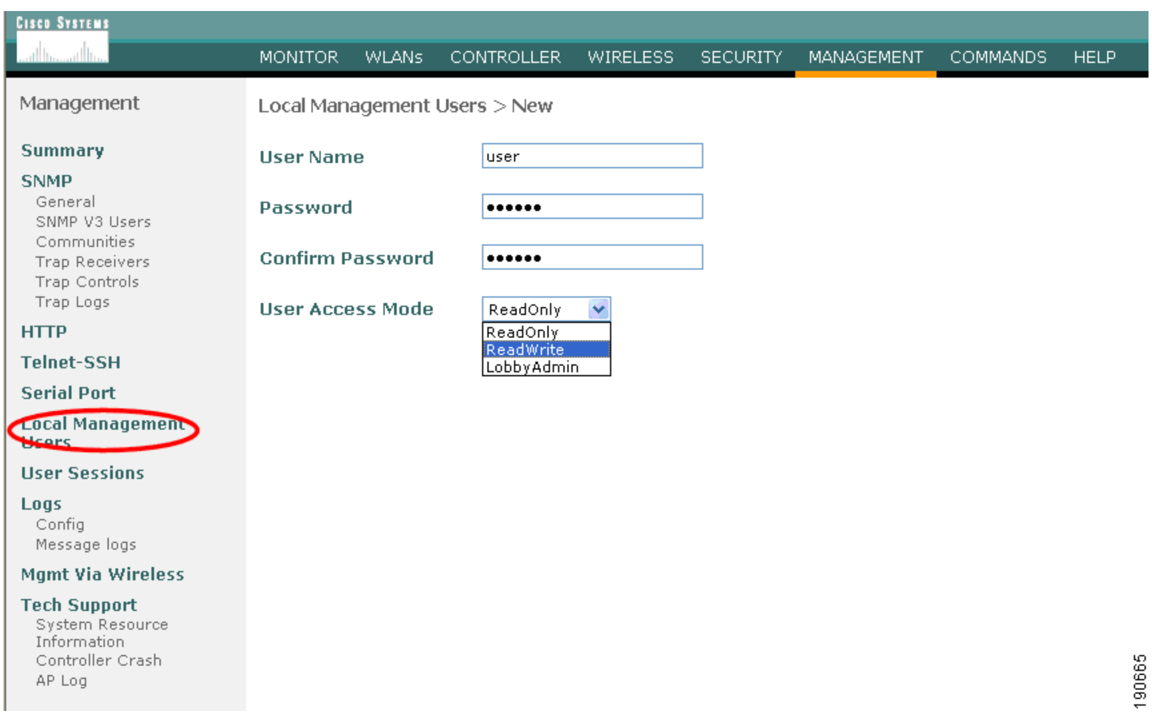
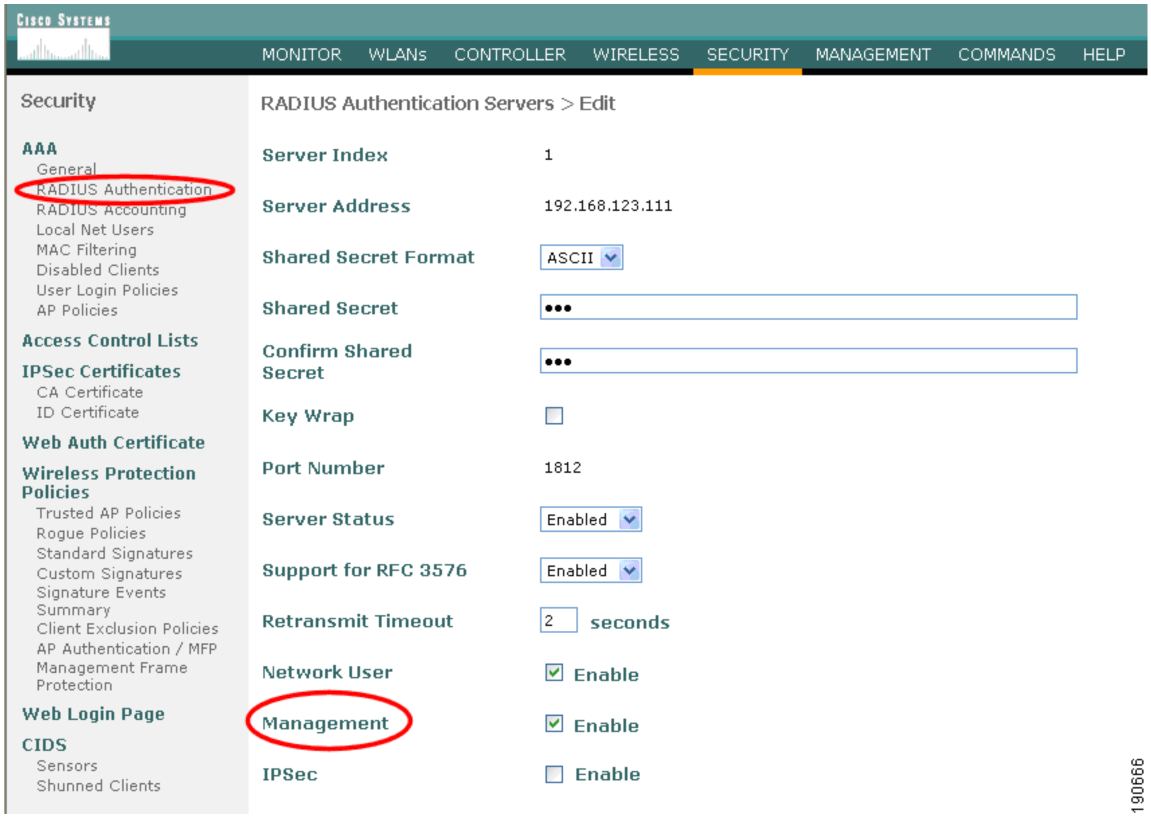


Figure 4-21 Management Users through RADIUS



WLAN LAN Extension

The goal of a WLAN LAN extension network is for the WLAN access network to transparently provide the same applications and services as the wired access network. Each WLAN extension topic covered in this section addresses the following types of transparency:

- Security transparency—Do the selected security capabilities provide seamless WLAN network security equivalent to wired networks?
- Application transparency—Are the supported WLAN network applications identical to applications on a wired network?
- Performance transparency—Does the WLAN deliver application performance that matches wired network performance?
- User transparency—Are users of the WLAN forced to perform network-specific operations to use the WLAN?

WLAN LAN Extension 802.1x/EAP

This section presents WLAN Extension 802.1x/EAP deployment in terms of the following key topics:

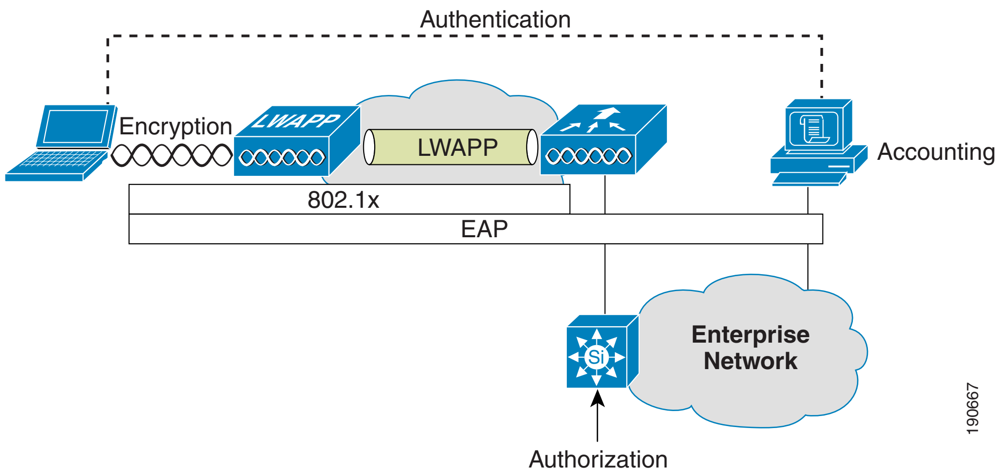
- Security transparency
- Application transparency
- Performance transparency
- User transparency

An 802.1x/EAP implementation of WLAN LAN Extension operates at the link layer (Layer 2) to provide authentication, authorization, accounting, and encryption. Figure 4-22 shows the 802.1x/EAP WLAN.

The security level provided is beyond that provided on most wired networks, providing link layer encryption and Authentication, Authorization, and Accounting (AAA) access control. This is provided as follows:

- Authentication occurs between the client and the authentication server. Several EAP types (LEAP, EAP-FAST, EAP-TLS, PEAP) are supported, allowing the enterprise to choose the authentication type that best suits its needs.
- Encryption is at the link layer between the WLAN client and the AP. The encryption keys are automatically derived during the authentication process. Note that the LWAPP messages between the LWAPP AP and the controller are encrypted; but the client data, although LWAPP encapsulated is not encrypted.
- Authorization is controlled by the VLAN or interface membership given to the wireless client in combination with the access controls applied at the access router or switch terminating the VLAN or interface.
- Accounting is provided by the RADIUS accounting communicated by the WLC to the RADIUS server.

Figure 4-22 WLAN LAN Extension 802.1X/EAP



Application Transparency

The Cisco Unified Wireless architecture creates a virtual access/distribution network through the LWAPP protocol that aggregates WLAN traffic at the WLC. After the WLAN client traffic leaves the WLC, it is the same as wired traffic: subject to the same access control, queuing, and routing. This achieves the WLAN LAN extension goal of supporting the same applications as the wired network. Any inability to run applications from the wired network over the WLAN network would be the result of policies or the fundamental limitations of the WLAN, and not because of the 802.1x/EAP architecture. Figure 4-22 shows the Cisco Unified Wireless operation.

Performance Transparency

A WLAN has a lower bit rate and a lower throughput than most enterprise wired LANs. Therefore, providing equivalent performance for all applications over the WLAN can be a challenge. The strategy to minimize differences in application performance between the wired and WLAN network is to use the QoS tools available on the WLAN and the APs. Those applications identified as being sensitive to network throughput and delay can be classified and scheduled as required. Load balancing and admission control tools on the WLAN can optimize the usage of the available WLAN resources. After the user or device has been authenticated, there is an opportunity to apply identity based on QoS features.

User Transparency

The various EAP types in 802.1x/EAP allow enterprises to choose an authentication mechanism that best matches security requirements. This allows the integration of the 802.1x/EAP into existing user behavior. Many organizations enforce stronger authentication mechanisms on their WLAN networks (compared to wired networks), because of reduced physical security in the WLAN. Stronger authentication enforcement on wired networks is expected to catch up with WLAN networks, with organizations using 802.1x/EAP mechanisms to enhance wired network security.

WLAN LAN Extension IPsec

The use of IPsec VPN tunnels is an alternative to an 802.1x/EAP implementation. Network designers might choose this implementation over an 802.1x/EAP solution because of security policy reasons. IPsec is a well-established standard that is endorsed by a number of security organizations. IPsec is a regulatory requirement in some industries.

The primary advantage of an IPsec-based VPN solution is the encryption mechanism. IPsec includes support of Triple Data Encryption Standard (3DES) and AES encryptions, and wide deployment experience.

A WLAN LAN extension that makes use of IPsec is generally considered more difficult to implement than an 802.1x/EAP based solution, but the Cisco Unified WLAN Architecture greatly simplifies this deployment style by allowing untrusted WLAN VPN client traffic to be sent to a centralized location through LWAPP, tunnels to a WLC, or aggregated to multiple WLCs to an anchor WLC through the mobility anchor feature.

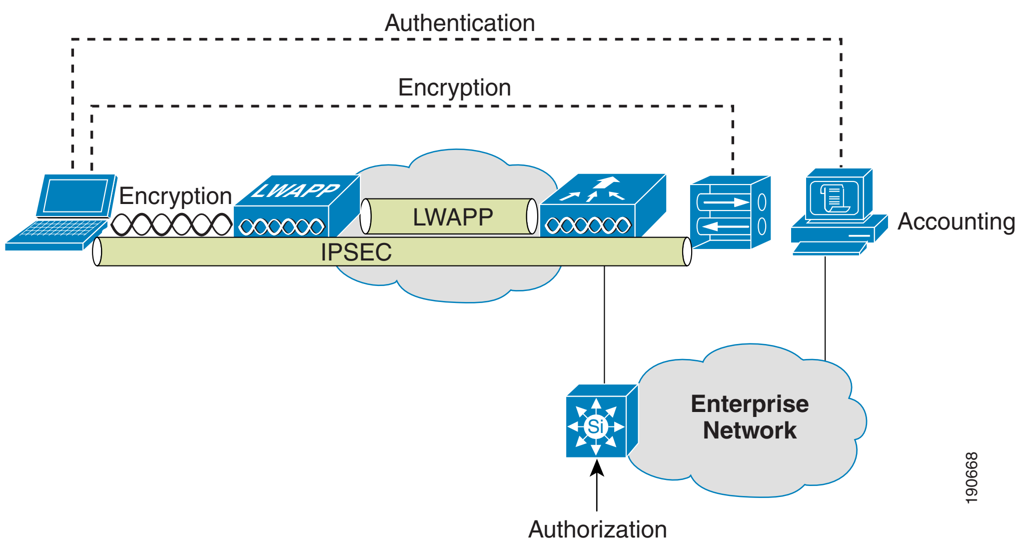
The network topology up to the VPN concentrator is considered untrusted, and an appropriate security policy must be created, configured, and maintained at all points that touch this untrusted network; for example, on the WLC, and the routers and switches between the WLC and the VPN concentrators. Some WLCs support VPN termination (440X model WLCs), and all WLCs can support VPN pass through, which is a mechanism to permit only VPN traffic destined for a external VPN concentrator on a certain WLAN.

Security Transparency

A WLAN LAN extension that uses IPsec provides AAA-equivalent features to that of 802.1x/EAP-based solutions (see Figure 4-23). Key elements are as follows:

- Authentication occurs between the client and the VPN concentrator. Multiple authentication types are supported within the IPsec framework.
- Encryption is at the network layer using 3DES or AES, and is negotiated between the client and the VPN concentrator. In addition to the inherent WLAN LAN extension IPsec security features associated with this implementation, VPN capabilities provide additional AAA-related security capabilities.
- Authorization is controlled by the VPN concentrator and is determined at the time of authentication. Policy is provided by the authentication server.
- Accounting is provided by RADIUS accounting software on both the VPN concentrator and the authentication server.

Figure 4-23 WLAN LAN Extension IPsec VPN



Application Transparency

As can be seen in Figure 4-23, WLAN traffic is transported over an IPsec tunnel to the VPN concentrator.

This can affect application transparency:

- Protocol limitations—Only the IP protocol is supported; the network is not multi-protocol
- Address translation—The IPsec client performs a form of address translation between its local IP address and that allocated by the VPN concentrator. This can impact the operation of some applications.
- No multicast—The connection to the VPN concentrator is point-to-point. Multicast applications are not supported.

Performance Transparency

Providing equivalent performance for all applications over the WLAN can be a challenge, because a WLAN has a lower bit rate and a lower throughput than most enterprise wired LANs. The use of IPsec VPN tunnels introduces some additional considerations:

- MTU size—The MTU size of packets must be adjusted to incorporate IPsec overhead.
- Processing overhead—Clients incur processing overhead from IPsec VPN. However, this should not be noticeable on most target platforms.
- Traffic classification and QoS considerations—Type of service (ToS) and differentiated services code point (DSCP) values are projected from client packets into the IPsec packets. As a result, QoS preference can be acted on, but no classification of traffic is possible while the traffic is IPsec encrypted.
- Traffic scheduling—All queuing at the VPN concentrator is handled on a first-in-first-out basis.

User Transparency

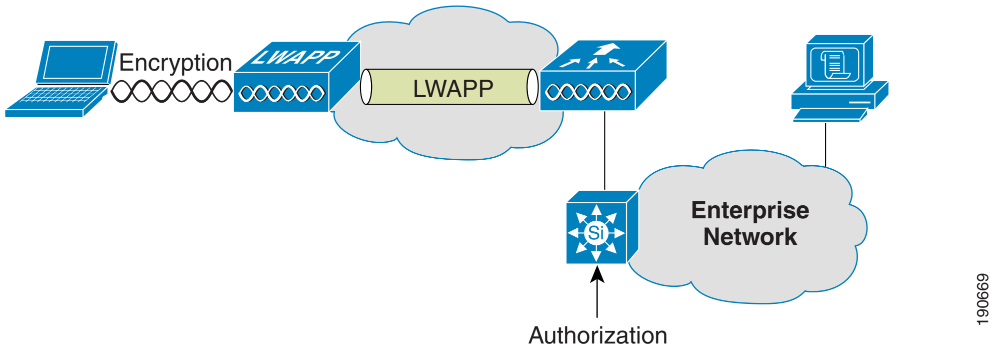
The Cisco IPsec VPN client has a number of features that aid user transparency, thereby providing an equivalent user experience when compared to that of 802.1x/EAP solutions:

- Auto Initiation—The VPN client can be configured to automatically launch for particular address ranges. In an enterprise, this would be configured to launch within the enterprise WLAN address ranges.
- OS Integration—The VPN client can capture user name and password information at login and use these as part of the VPN client login. This is similar to the process used in EAP-Cisco. As an alternative, the VPN client can use stored certificates associated with a specific user, similar to EAP-TLS. These features coupled with Auto Initiation should provide a high level of user transparency.

WLAN Static Keys

Static key implementations are not recommended for general purpose WLAN LAN extension networks because of known weaknesses in the WEP encryption algorithms, and because of the difficulty in the configuration and maintenance of static keys for WEP or other stronger encryption schemes. Certain client devices are capable of supporting static WEP keys only (see Figure 4-24). These clients should be put on a separate WLAN VLAN or interface and have their authorization limited to addresses and protocols specific to the application supported by the Static WEP client. If possible, WPA-PSK or WPA2-PSK should be used in place of WEP because these mechanisms address the known weaknesses in the WEP encryption system

Figure 4-24 WLAN Static WEP Keys



Security Transparency

Some security issues related to static key implementations are as follows:

- Weak authentication—Any hardware device with a matching configuration and key can join the network. The Static key authenticates a group of devices, never individual users. MAC filtering can be added, but MAC addresses are sent in the clear, and can be spoofed.
- Encryption limitation—Encryption is at the link layer between the WLAN client and the AP. The current encryption mechanisms available are WEP, WPA-PSK, or WPA2-PSK. If possible, WPA-PSK or WPA2-PSK should be used.
- Authorization limitation—Authorization is controlled by the VLAN membership associated with the SSID, or assigned through MAC filtering.
- Accounting is not available.

Application Transparency

As illustrated in Figure 4-24, the WLAN connects at the access/distribution layer. When the WLAN client traffic leaves the WLC, it is the same as wired network traffic and subject to the same access control, queuing, and routing. WLAN Static key solutions should be limited to the specialized applications that the Static WEP client supports. The network would appear transparent to this application, but to all other applications access should be blocked.

Performance Transparency

To minimize differences in application performance between the wired and WLAN network, use the QoS tools available on the WLAN, the APs, and WLC. Those applications identified as being sensitive to network throughput and delay can be classified and scheduled as required. Load balancing and admission control tools on the WLAN can optimize the usage of the available WLAN resources. Because Static WEP performs no user authentication, no user-based QoS policies can be applied, but MAC-based QoS policies are possible.

User Transparency

Static WEP requires no authentication and should be transparent to the supported applications and users. The static WEP key becomes an issue only for the user if required to change it.

Cisco Unified WLAN Architecture Considerations

The Cisco Unified WLAN architecture has features that can enhance solution transparency. The following section details some of the specific considerations. For more information, see the following URL: http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/emob41dg/ch4_Secu.html.

Security Transparency

The features offered by Cisco Unified WLAN architecture do not directly impact security transparency because the architecture supports all the existing security models. An integrated WLC solution, such as WISM, can make it easier to implement various security solutions through integration with IOS features on that platform.

Application Transparency

PKC and CCKM enable WLAN clients to quickly roam between APs. The WLC caches session credentials (security keys) derived for a client session and uses them for re-authentication and re-keying when a client roams, within the mobility group. Caching this information rather than forcing the client to do a full authentication reduces the authentication time and therefore the total time required for roaming. This can enhance application transparency because the impact of roaming is reduced and less likely to impact either the application or the user.

Performance Transparency

The Cisco Unified WLAN Architecture has been designed to use and maintain the QoS features used in neighboring wired networking platforms.

User Transparency

Cisco Unified WLAN Architecture is compatible with all other WLAN client solutions, and therefore does not have an adverse impact on user transparency.

Note Cisco Unified WLAN architecture is compatible with CCXv4 with the 4.0 controller software release.

EAP Considerations for High Availability ACS Architecture

As a centralized authentication server, Cisco Secure ACS introduces RADIUS-based AAA capabilities to an enterprise network for both wired and WLAN networks. Implementing ACS redundancy and reliability is meant to address two issues:

- The ACS server should not represent a single point of failure.
- A network failure should not impact a user's ability to log on.

The first issue is a good reason to replicate the ACS database to a secondary server, allowing for failover and maintenance. This redundancy configuration should be implemented in almost all cases. The second issue is an instance in which it is critical to use the local WLAN even in the event of a network failure preventing access to a remote ACS server. Implementation of this second use of replication depends on the application architecture of the enterprise. For example, if the applications that the users want to reach are also remote, little is to be gained by being able to use the WLAN.

One issue that should also be considered in RADIUS planning is the impact that WAN latency can have on authentication. This is especially true in (non key caching) re-authentication scenarios where a full authentication back to the RADIUS server is required when a client roams between APs and thereby adds latency to the client roam. In cases where clients roaming times need to be minimized, key-caching mechanisms such as PKC or CCKM should be considered. These mechanisms have the advantage of requiring full RADIUS authentication only initially and using the cached key when a client roams, reducing the client roam times, and reducing the load on the WAN and RADIUS server.

ACS Architecture

The ACS deployment strategy must consider how the entire enterprise identity system will be structured, rather than just the campus. A key consideration is the location of directory databases. It is essential that the ACS strategy reflect an approach in which the elements of the ACS architecture are carefully analyzed, designed, and implemented for authentication systems associated with the directory architecture of the organization. The assessment of the directory architecture is the starting point for the ACS deployment strategy. In an ideal situation, the existing infrastructure can provide the user names, passwords, and profiles to the ACS servers. That is, the ACS acts as a AAA interface between users and the directory system, and placement of ACS servers needs to align with the placement of directory resources.

In deploying multiple ACS servers, the ACS replication service can be used to replicate a master ACS with slave ACSs in the network (the replication is master/slave).

Sample Architecture

Figure 4-25 shows an example of what ACS architecture might look like. Campus A holds the authoritative ACS database server. This server is replicated to the other enterprise ACS servers. WLCs communicate to the two local ACS servers.

Campus B, because of its size and distance from Campus A, has opted for another two ACS servers, thus providing its own backup. Campus C, being smaller and closer to Campus A, has opted to have only one server, and relies on Campus A for backup. The branch offices use the ACS servers that are the shortest network distance from them.

Figure 4-25 Sample ACS Architecture