CHAPTER 1

802.11 Network Security Fundamentals

This chapter provides an overview of the 802.11 network security features and contains these sections:

Introduction

This section is intended for system administrators planning an enterprise wireless LAN deployment and provides an overview of the main 802.11 security features currently available. The chapter focuses on Wi-Fi Protected Access (WPA) and WPA2, but also briefly covers the older Wired Equivalent Privacy (WEP) feature.

WEP is the initial security mechanism specified in the original 802.11 standard and was superseded by the 802.11i standard update. The 802.11 standard initially had security flaws that were resolved with the introduction of the 802.11i standard update. These new security enhancements address the enterprise requirements for confidential communications through the use of authentication and encryption.

Terminology

This document uses a number of common terms for basic physical components in the wireless system. Figure 1-1 illustrates the system topology of these components: the wireless LAN client, access point, wireless LAN controller (WLC), and AAA (authorization, authentication, and accounting) server.

Figure 1-1 Secure Wireless Topology

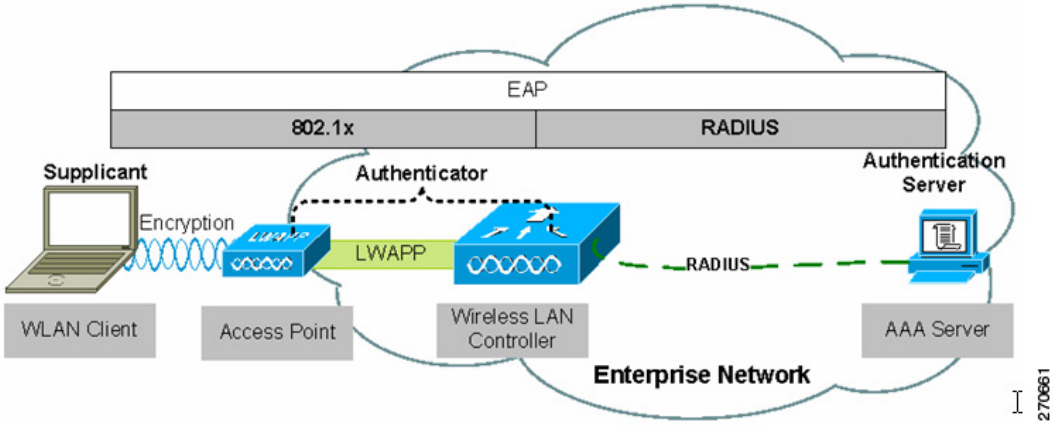


Figure 1-1 also illustrates the basic roles and relationships of the 802.1X authentication process. The 802.1X supplicant (Cisco Secure Services Client) resides on the wireless LAN client, the access point and the WLC, through the split-MAC architecture, act as the 802.1X authenticator, and the AAA server is the authentication server. This figure also illustrates the role of 802.1X and the RADIUS protocol in carrying EAP (Extensive Authentication Protocol) packets between the client and the authentication sever. For additional information on 802.1X, refer to the "IEEE 802.1X" section on page 1-6 . For additional information on EAP, refer to the "EAP" section on page 1-7.

IEEE 802.11 Fundamentals

An 802.11 wireless LAN consists of the following basic components and behaviors:

- Beacons—Used to indicate the presence of a wireless LAN network.
- Probe—Used by wireless LAN clients to find their networks.
- Authentication—A feature defined in the original 802.11 standards.
- Association—The process of establishing a link between an access point and a wireless LAN client.

Beacons are regularly broadcast by an access point, but the probe, authentication, and association frames are generally only used during the association and reassociation processes.

Beacons

The wireless LAN beacon frame contains configuration information about the access point, such as the SSID (service set identifier or the network name), the supported bit rates, and the security configuration for that wireless LAN.

The primary purpose of the beacon is to allow wireless LAN clients to know what networks are available in the area. This allows the wireless LAN clients to choose a network to try to associate with.

Many wireless LAN security documents suggest that sending beacons without the SSID is a security best practice, to help prevent potential hackers from learning the SSID. All enterprise wireless LAN solutions offer this capability as an option, but this option has little value because the SSID can be easily discovered during an association attempt. Also some wireless LAN clients rely upon the SSID

information in the beacon and do not reliably associate with wireless LANs that do not advertise the SSID information. For these reasons, it is best to allow the SSID information to be broadcast in the beacon.

Association—the Join Process

With the exception of fast roaming, an 802.11 client must go through a three-stage process before being allowed to send data over a wireless LAN network:

1. Find a suitable wireless LAN network—For an enterprise deployment, the search for a suitable network involves the sending of a probe request on multiple channels and specifying the network name (SSID), bit rate requirements, and required security configuration.
2. 802.11 authentication—802.11 supports two authentication mechanisms: open authentication and shared key authentication. Open authentication is fundamentally a NULL authentication in which the client requests to be authenticated and the access point responds positively. The 802.11 shared WEP key authentication implementation is flawed, but it must be included for compliance with the standards. Shared key authentication is not recommended and should not be used.

   Open authentication is the only mechanism used in enterprise wireless LAN deployments. As previously indicated, open authentication is fundamentally a NULL authentication, and the real authentication occurs after association through the 802.1X and EAP authentication mechanisms.
3. 802.11 associations—This stage finalizes the security and bit rate options and establishes the data link between the wireless LAN client and the access point. A secure enterprise wireless LAN access point blocks all of the wireless LAN client traffic at the access point until a successful 802.1X authentication. If a client has joined a network and roams from one access point to another network the association is called a *reassociation*. The primary difference between an association and a reassociation is that a reassociation sends the basic MAC address (BSSID) of the previous access point in the reassociation request to provide roaming information to the extended network.

Probe Request and Probe Response

SSC can be configured with the wireless LAN networks, which enables the wireless LAN client to send a probe request that contains the SSID of the desired wireless LAN network.

If the wireless LAN client is trying to discover the available wireless LAN networks, it can send out a probe request without an SSID. When this occurs, all access points that are configured to respond to this type of query send a probe response. Wireless LANs without broadcast SSID enabled do not respond.

Association

The association and association response frames provide the final agreement for the data rates and security settings. After this process is completed, 802.11 data frames can be sent between the wireless LAN client and the wireless LAN access point. In an enterprise wireless LAN deployment, these data frames are limited to 802.1X frames between the wireless LAN client and the access point until the 802.1X or EAP authentication is completed and successful.

The association process also has a related disassociation frame used to disconnect a wireless LAN client from its access point. The disassociation frame can only be a unicast frame.

Reassociation

Reassociation occurs when a wireless client temporarily moves out of range of an access point or roams to another access point. The reassociation process is similar to the association process, except that when roaming is involved, the new and old access points communicate on the wired network to move wireless client information between each other.

When the wireless client roams to a new access point, the reassociation process is used to inform the 802.11 network that the client has moved to a new location. The wireless client issues a reassociation frame to the new access point, which identifies the old access point. The new access point communicates with the old access point over the wired link to verify that the wireless client was previously associated. If the wireless client was previously associated, the new access point issues a reassociation response frame to the wireless client; otherwise, it issues a disassociation frame. After sending the reassociation response, the new access point contacts the old access point over the wired link to complete the reassociation process. Any buffered frames at the old access point are transferred to the new access point. After completing the reassociation process, the new access point begins processing frames from the wireless client.

Authentication

As previously stated, there are two 802.11 authentication modes: open-mode and shared-mode. 802.11 authentication alone provides only nominal security and is mostly used in a home wireless network in which network security is not a major concern. Home users who need to join their enterprise networks using access points that are not configured for 802.1X must establish a VPN connection using SSC. For more information on VPN, refer to the "VPN Integration" section on page 2-31.

Another frame type related to authentication frames is the deauthentication frame. When a deauthentication frame is received by a wireless LAN client, the client is disconnected from the access point. This might cause a wireless LAN client to go through the entire probe request process again or cause the client to restart the authentication association process again. Deauthentication frames can be sent to the broadcast MAC address.

Wireless Network Security Concepts

Security should be considered a network design component that needs to be integrated and not something that is added later. Security also needs to be subjected to the same cost/benefit analysis and usability considerations as the rest of the network components.

Enterprise security discussions consistently indicate that the wireless LAN's RF signals typically travel beyond the deployed building's perimeter. This allows the network to be monitored and attacked from beyond the property line. However, the range for this type of attack is very limited. To make any attack feasible an attacker with the appropriate skills needs to be in physical proximity to a wireless LAN. This requires the attacker to roam extensive areas looking for a suitable wireless LAN. An 802.1X framework for access control coupled with other wireless environment management tools can severely restrict the feasibility of such attacks. The location of an enterprise, and the type of business operated by that enterprise, will determine any recommended augmentation of the native wireless LAN security.

Physical Security

Hostile activities are equally applicable to all networks and can be broadly broken down into:

- Intelligence gathering—Normally aids in gaining unauthorized access to enterprise resources but can be for other reasons, such as to determine the location of key individuals or activity. The choice of EAP type used in authentication and the configuration of the supplicant can determine whether username information is exposed during authentication.
- Unauthorized access—The authentication and encryption in 802.11 security can protect sessions, but policies and processes do need to be in place to protect equipment and passwords. This is generally addressed in two ways:
  - End node security to protect mobile devices not directly related to the wireless LAN. This type of security needs to be assessed with a understanding of the end node's mobility.
  - WPA or WPA2 for wireless LAN clients that provides authentication of users and confidentiality of user communication over the wireless LAN.
- Denial of service—A wireless LAN network attack that prevents legitimate wireless users from accessing information or services on the network. This attack typically uses 802.11 management frames or RF interference in the same spectrum as the wireless LAN network. This type of attack is addressed through RF management and wireless IDS features (WIDS).

Regulation, Standards, and Industry Certifications

Most network system standards are typically from the Institute of Electrical and Electronic Engineers (IEEE) and the Internet Engineering Task Force (IETF). The two core standards introduced in secure wireless LAN deployment are the 802.11 standards defined by the IEEE and the EAP standards defined by the IETF.

IEEE

The IEEE owns the 802.11 group of standards. The original 802.11 standard was published in 1999 and there have been a number of amendments to the standard. These amendments have added different physical layer implementations, provided greater bit rates (802.11b, 802.11a, and 802.11g), added quality of service (QoS) enhancements (802.11e), and added security enhancements (802.11i).

The IEEE also owns the 802.1X standard for port security that is used in 802.11i for authentication of wireless LAN clients.

IETF

The main IETF Request For Comments (RFCs) and drafts associated with wireless LANs are based upon the Extensible Authentication Protocol (EAP). The advantage of EAP is that it decouples the authentication protocol from its transport mechanism. EAP can be carried in 802.1X frames, PPP frames, UDP packets, and RADIUS packets.

EAP is carried over the wireless LAN in 802.1X frames and in RADIUS packets between the access points and the AAA server. This provides an end-to-end EAP authentication between the wireless LAN client and the AAA server. See the "EAP" section on page 1-7.

Wi-Fi Organization

In wired networks it is common for devices to be from the same vendor where integration is part of product testing. When different vendor devices are combined into the same network, interoperability and integration must be managed and controlled by a group of network specialists who understand the devices and their interaction.

In wireless networks that include devices from many vendors, the wireless standards allowed different interpretations and optional features to be developed. A group of industry companies and organizations formed the Wi-Fi Alliance (www.wi-fi.org) to certify wireless LAN interoperability through WPA, WPA2, and Wi-Fi Multimedia (WMM) certification programs.

The WPA standard was developed to address the weakness in the WEP encryption process prior to the ratification of the 802.11i work group standard. One of the key development goals was to make it backward compatible with WEP hardware. This allowed the continued support of the base RC4 encryption used in WEP, but added keying enhancements and message integrity check improvements that addressed the weaknesses in WEP encryption.

WPA2 is based upon the ratified 802.11i standard and uses AES-CCMP encryption. This encryption requires new client and access point hardware. Due to the long upgrade cycles for laptops and client devices, a mixed WPA and WPA2 environment will exist for some time. In a greenfield enterprise deployment (without constraints imposed by prior implementations), it is expected that customers will be able start with WPA2.

Cisco Compatible Extensions

The Cisco Compatible Extensions (CCX) program ensures the widespread availability of wireless client devices that are compatible with a Cisco wireless LAN infrastructure and take advantage of Cisco innovations for enhanced security, mobility, quality of service, and network management.

IEEE 802.1X

IEEE 802.1X is an IEEE standard framework for port based access control that has been adopted by the 802.11i security workgroup as the means of providing authenticated access to wireless LAN networks.

- The 802.11 association process creates a virtual port for the wireless LAN client on the access point.
- The access point blocks all data frames apart from 802.1X traffic.
- The 802.1X frames carry the EAP authentication packets, which are passed through to the AAA server by the access point.
- If the EAP authentication is successful, the AAA server sends an EAP-success message to the access point. The access point then allows data traffic from the wireless LAN client to pass through the virtual port.
- Prior to opening the virtual port, data link encryption was established between the wireless LAN client and the access point. This ensures that another wireless LAN client cannot access the port that has been opened for the authenticated client.

EAP

EAP is an IEFT RFC that addresses the requirement for an authentication protocol to be decoupled from the transport protocol carrying it. This allows the EAP protocol to be carried by transport protocols, such as 802.1X, UDP, or RADIUS without changes to the authentication protocol.

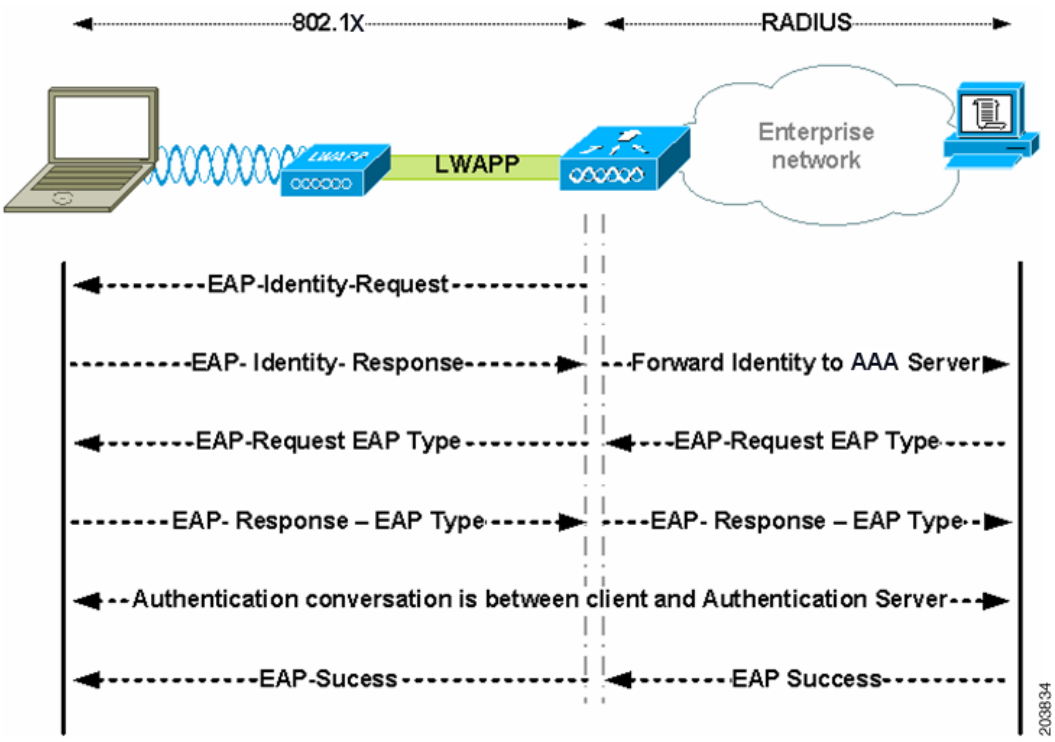
The basic EAP protocol is relatively simple and made up of four packet types:

- EAP request—The authenticator sends the request packet to the supplicant. Each request has a type field that indicates what is being requested, such as the supplicant identity and EAP type to be used. A sequence number allows the authenticator and the peer to match an EAP response to each EAP request.
- EAP response—The supplicant sends the response packet to the authenticator and uses a sequence number to match the initiating EAP-request. The type of the EAP response generally matches the EAP request, unless the response is a NAK.
- EAP success—The authenticator sends the success packet upon successful authentication to the supplicant.
- EAP failure—The authenticator sends the failure packet upon unsuccessful authentication to the supplicant.

When EAP is in use in an 802.11i system, the access point is operating in an EAP pass-through mode. In this mode, the access point checks the code, identifier, and length fields and then forwards the EAP packets received from the supplicant to the AAA server. Packets received from the AAA server at the authenticator are forwarded to the supplicant.

Figure 1-2 illustrates the EAP protocol messages.

Figure 1-2 EAP Protocol Flow



EAP-FAST

EAP-FAST is a Cisco proprietary 802.1X authentication type that offers flexible, easy deployment and management, supports a variety of user and password database types, supports server-initiated password expiration and change, and a digital certificate (optional).

EAP-FAST was developed for customers who want to deploy an 802.1X EAP type that does not use certificates and provides protection from dictionary attacks.

EAP-FAST encapsulates TLS messages within EAP and consists of three protocol phases:

1. A provisioning phase that uses Authenticated Diffie-Hellman Protocol (ADHP) to provision the client with a shared secret credential called a Protected Access Credential (PAC).
2. A tunnel establishment phase in which the PAC is used to establish the tunnel.
3. An authentication phase in which the authentication server authenticates the user's credentials (token, username/password, or digital certificate).

EAP-TLS

EAP-Transport Level Security (EAP-TLS) is an 802.1X EAP authentication algorithm based on the TLS protocol (RFC 2246). TLS uses mutual authentication based on X.509 digital certificates. The EAP-TLS message exchange provides mutual authentication, cipher suite negotiation, and private key exchange and verification between the client and the authenticating server.

The list below indicates the main reasons why using EAP-TLS client certificates provides strong authentication for wireless connections:

- Authentication occurs automatically, usually with no intervention by the user.
- Does not require dependency on a user password.
- Uses digital certificates for strong authentication protection.
- Message exchange is protected with public key encryption.
- Not susceptible to dictionary attacks.
- The authentication process results in a mutually determined key for data encryption and signing.

EAP-TTLS

EAP-Tunnelled Transport Layer Security (EAP-TTLS) is a two-phase protocol that expands the EAP-TLS functionality. Phase 1 conducts a complete TLS session and derives the session keys used in Phase 2 to securely tunnel attributes between the server and the client. The attributes tunneled during Phase 2 can be used to perform additional authentications using a number of different mechanisms.

The authentication mechanisms that can be used during Phase 2 include these protocols:

- PAP (Password Authentication protocol)—Uses a two-way handshake to provide a simple method for the peer to establish its identity on initial link establishment.An ID/Password pair is repeatedly sent by the peer to the authenticator until authentication is acknowledged or the connection is terminated.
- CHAP (Challenge Handshake Authentication Protocol)—Uses a three-way handshake to periodically verify the identity of the peer.

- MS-CHAP (Microsoft CHAP)—Uses a three-way handshake to periodically verify the identity of the peer.
- MS-CHAPv2—Provides mutual authentication between peers by including a peer challenge in the response packet and an authenticator response in the success packet.
- EAP—Allows use of these EAP methods:
  - EAP MD5 (EAP-Message Digest 5)—EAP-MD5 is an EAP security algorithm that uses a 128-bit generated number string, or hash, to verify the authenticity of the data packets.
  - EAP MSCHAPv2—Uses a three-way handshake to periodically verify the identity of the peer.

EAP-PEAP

EAP-PEAP is an 802.1X EAP authentication type that takes advantage of server-side EAP-TLS and supports a variety of different authentication methods, including certificates, tokens, logon passwords, and one-time passwords (OTPs).

EAP-PEAP protects the EAP methods by providing these services:

- Creates a TLS tunnel for the EAP packets
- Message authentication
- Message encryption
- Authentication of server to client
- Key exchange to establish dynamic WEP or TKIP keys

These authentication mechanisms can be used:

- Password
  - EAP MSCHAPv2—Uses a three-way handshake to periodically verify the identity of the peer.
  - EAP GTC (EAP Generic Token Card)—Defines an EAP envelope to carry the user password.
- Token
  - EAP GTC—Defines an EAP envelope to carry a user OTP generated by a token card.
- Certificate
  - EAP TLS—Defines an EAP envelope to carry the user certificate.

Authentication

Depending upon the customer requirements, different authentication mechanisms are used in a secure mobility environment, but all of the mechanisms use 802.1X, EAP, and RADIUS as their supporting protocols. These protocols allow access to be controlled based upon the successful authentication of the wireless LAN client and allows the wireless LAN network to be authenticated by the user.

This system also provides the other elements of AAA, authorization and accounting, through policies communicated through RADIUS and RADIUS accounting.

The mechanism for performing authentication is described in more detail in the following sections, but the primary factor affecting the choice of authentication protocol is integration with the current client authentication database. A secure wireless LAN deployment should not require the creation of a new authentication system for users.

Supplicants

The software clients used for 802.1X authentication are generally called *supplicants* and are based upon 802.1X terminology. SSC is a supplicant for wired and wireless networks. It supports a number of different EAP methods that map appropriately to different authentication system requirements of customers. Common EAP methods supported by SSC are listed below:

- Protected EAP (PEAP) MSCHAPv2—Uses a Transport Layer Security (TLS) tunnel to protect an encapsulated MSCHAPv2 exchange between the wireless LAN client and the authentication server.
- PEAP GTC (Generic Token Card)—Uses a TLS tunnel to protect a generic token card exchange.
- EAP-Flexible Authentication via Secured Tunnel (FAST)—Uses a tunnel to protect the exchange.
- EAP-TLS—Uses mutual authentication based on X.509 digital certificates.

Table 1-1 lists a summary of common EAP methods:

Table 1-1 Feature Comparison of EAP Methods with Cisco SSC

Feature	Cisco EAP-FAST	PEAP MS-CHAP v2	PEAP EAP-GTC	EAP-TLS
Single sign-on (Microsoft Active Directory only)	Yes	Yes	Yes	Yes
Login scripts (Microsoft Active Directory only)	Yes	Yes	Some	Yes
Password change (Microsoft Active Directory only)	Yes	Yes	Yes	–
Microsoft Active Directory database support	Yes	Yes	Yes	Yes
Access Control Server (ACS) local database support	Yes	Yes	Yes	Yes
Lightweight Directory Access Protocol (LDAP) database support	No	No	Yes	Yes
One-time-password (OTP) authentication support	No	No	Yes	No
RADIUS server certificate required	Yes	Yes	Yes	Yes
Client certificate required	No	No	No	Yes
Anonymity	Yes	Yes	Yes	No

Authenticator

The authenticator in the Cisco Secure Mobility Solution is the WLC that processes the incoming 802.1X frames from the wireless LAN access points, and acting in EAP pass-through mode, it relays the EAP packets to and from the 802.1X frames and the RADIUS packets.

Upon the completion of a successful authentication, the WLC receives a RADIUS packet that contains an EAP success message, an encryption key that was generated at the authentication server during the EAP authentication, and RADIUS extensions for communicating policy.

Refer to Figure 1-1 to see the location of the authenticator within the overall authentication process. The authenticator controls network access through the 802.1X mechanism and relays EAP messages between the supplicant and the authentication server.

Authentication Server

The authentication server used in the Cisco Secure Mobility Solution is the Cisco Access Control Server (ACS). Cisco ACS is available as software installable on a Windows 2000 or 2003 server or as an appliance. The authentication server can also be embedded into wireless LAN infrastructure devices; for example, it could be the local authentication services on an access point running Cisco IOS software or the AAA services included in the Cisco WLSExpress.

The authentication server performs the EAP authentication over a RADIUS tunnel.

Upon the completion of a successful EAP authentication, the authentication server sends an EAP success message to the authenticator. This message tells the authenticator that the EAP authentication process was successful and passes the Pairwise Master Key to the authenticator. The master key is used to create the encrypted stream between the wireless LAN client and the access point.

Encryption

There are two enterprise level encryption mechanisms specified in 802.11i: WPA and WPA2. These encryption types are Temporal Key Integrity Protocol (TKIP) and Advanced Encryption Standard (AES).

TKIP, the encryption certified in WPA, provides support for legacy wireless LAN equipment by addressing the flaws in WEP while still supporting the core encryption algorithm (RC4). The hardware refresh cycle of the client devices is such that TKIP is likely to be a common encryption mechanism for a number of years. While TKIP addresses all the known weaknesses of WEP, the AES encryption of WPA2 is the recommended encryption mechanism because it brings the wireless LAN encryption into alignment with current encryption best practice.

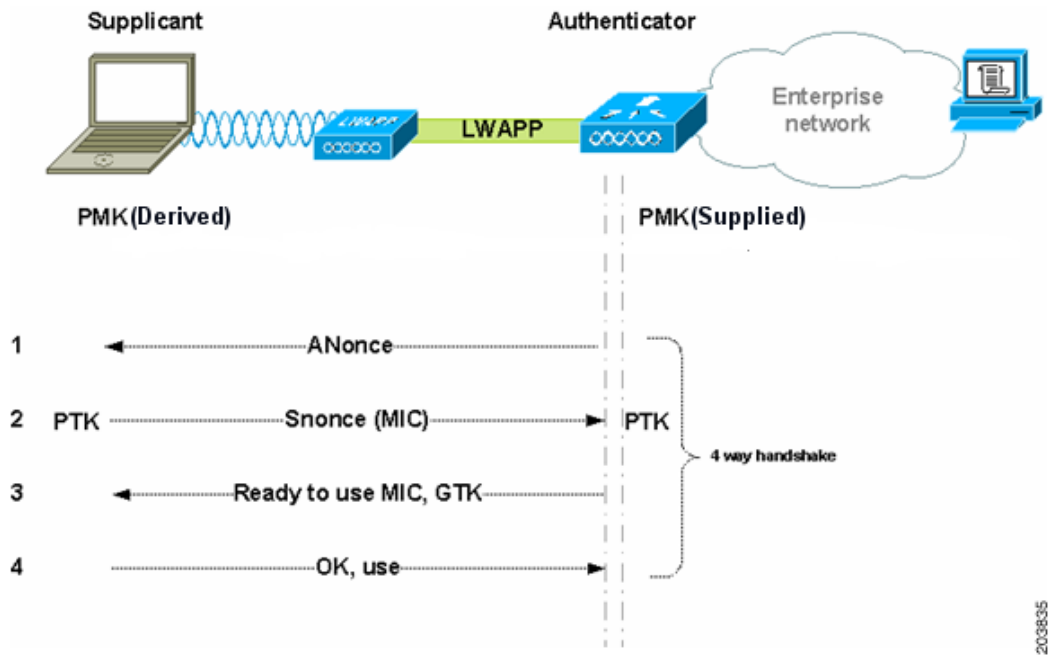
The two primary mechanisms in TKIP are the generation of a per packet key for RC4 encryption of the MSDU (MAC Service Data Unit) and an additional Message Integrity Check (MIC) for the encrypted packet.

AES Counter Mode/CBC MAC Protocol (CCMP) is the AES encryption mode used in 802.11i in which the counter mode provides confidentially and CBC MAC provides message integrity.

Four-Way Handshake

The four-way handshake describes the mechanism used to derive the encryption keys used to encrypt wireless data frames. Figure 1-3 shows a schematic of the frame exchanges used to generate the encryption keys. These keys are referred to as *temporal keys*.

Figure 1-3 Four-Way Handshake



The keys used for encryption are derived from the Pairwise Master Key (PMK) that has been mutually derived during the EAP authentication section. This PMK is sent to the authenticator. The PMK is not forwarded to the supplicant because the supplicant has derived its own copy of the PMK.

The four-way handshake consists of these events:

1. The authenticator sends an EAPOL-Key frame containing an ANonce (Authenticator Nonce—a random number generated by the authenticator).
   - The Supplicant derives a Pairwise Temporal Key (PTK) from ANonce and SNonce (Supplicant Nonce—a random number generated by the authenticator).
2. The supplicant sends an EAPOL-Key frame containing SNonce, the RSN information element from the reassociation request frame, and a Message Integrity Check (MIC).
   - The authenticator derives PTK from ANonce and SNonce and validates the MIC in the EAPOLKey frame.
3. The authenticator sends an EAPOL-Key frame containing ANonce, the RSN information element from its beacon or probe response messages, MIC, whether to install the temporal keys, and the encapsulated Group Temporal Key (GTK—the multicast encryption key).
4. The supplicant sends an EAPOL-Key frame to confirm that the temporal keys are installed.

Seamless Connectivity

To achieve wireless mobility, the network administrator needs to perform a site survey to ensure that the enterprise premise has adequate wireless coverage. Cisco provides wireless spectrum analysis tools and applications that help achieve a balanced and well-designed wireless infrastructure.

Enterprise network infrastructures are based on both wired and wireless media in which wireless media provide better mobility and wired media often provide much greater speeds and throughput. Both wired and wireless connections should be able to restore mapped network drives, run log-on scripts, execute computer group policy objects (GPOs) and user GPOs, and perform tasks that require network connections when a user logs in to a wireless LAN client PC or reboots. In addition, the wireless LAN client should be able to restore connectivity after resuming from a client suspension or hibernation.

Most enterprise environments require that end users be able to have connectivity when they undock their workstations or detach the Ethernet cable and move to another location, such as a conference room. In a typical enterprise, a lack of connection is acceptable while the user is in transit. However, when he arrives at the new location, he should be able to easily regain connectivity. Other enterprises may require connectivity while in transit as they may have application that may require continuous connectivity such as Voice-over-IP (VoIP) applications. Wireless roaming addresses these concerns in a wireless network infrastructure.

Roaming

The end user should be able to:

- Easily switch from a wired connection to a wireless connection and back again.
- Roam from one access point with a lower signal strength to another access point with a better signal strength that has the same SSID.

Roaming from one access point to another requires a disassociation with the previous access point and an association with the new access point. This process leads to a termination of existing network connections, especially in an enterprise environment that requires 802.1X. Roaming is followed by an 802.1X authentication. This whole process may take 30 seconds or more.

Session resumption reduces the reconnection time during an 802.1X reauthentication provided that EAP-TLS, EAP-FAST, or EAP-PEAP is the deployed authentication method.

Session Resumption

A typical EAP-TLS handshake takes many packet exchanges before an EAP success message is generated, which is followed by a four-way handshake to establish the encryption keys. When using a centralized backend authentication server, session resumption provides a simpler authentication handshake when roaming to a new access point by leveraging session state information from the user's previous authentication session. This reduces the number of the handshake packet exchanges.

Although this action reduces the time for reconnection, it still does not suffice for real-time application such as Voice-over-IP (VoIP) running on the wireless LAN client that require the reconnection time to be between 50 and 200 ms.

The wireless network framework supports fast secure roaming where authenticated client devices can roam securely from one access point to another without any perceptible delay during reassociation. Fast secure roaming also supports latency-sensitive applications such as wireless VoIP.

Fast Secure Roaming

Fast roaming is most pertinent for hand-held devices using Wi-Fi applications dealing with real-time data. There are two main techniques that help achieve fast roaming: Cisco's CCKM and 802.11i PMKID caching.

In both the approaches, the wireless infrastructure pre-establishes the needed key material that was previously derived from 802.1X authentication for the neighboring access points.

Once connected to an access point, 802.11i PMKID caching allows the list of neighboring access points to be shared with the wireless LAN client, and then 802.11i PMKID tunnels the 802.1X authentication (referred to as pre-authentication) between other access points and the wireless LAN client over the existing wireless connection. When the wireless LAN client actually roams from one access point to another, it looks up its neighboring access point and uses the applicable PMK to perform just the four-way handshake to establish connectivity after association.

CCKM uses a different method. If the wireless network infrastructure is based on Cisco access points, the wireless LAN client can avoid a pre-authentication and a four-way handshake so that fast roaming is achieved during reassociation to another Cisco access point.