# Deploying Wi-Fi Protected Access (WPA™) and WPA2™ in the Enterprise

March 2005

**TABLE OF CONTENTS**



## Executive Summary

By 2001, a series of independent studies from various academic and commercial institutions had identified weaknesses in Wired Equivalent Privacy (WEP), the original native security mechanism for wireless local area networks (WLANs) in the Institute of Electrical and Electronics Engineers (IEEE) 802.11 specification. These studies showed that, even with WEP enabled, an intruder equipped with the proper tools and a moderate amount of technical knowledge could gain unauthorized access to the wireless network via the WLAN. As a result, enterprises found it necessary to supplement WEP with third-party security solutions such as VPN, IEEE 802.1X authentication services servers, or add-on proprietary technologies.

To address this situation, Wi-Fi® Alliance introduced 2 new interoperable Wi-Fi security specifications for both enterprise and home networks.

In 2003, the Wi-Fi Alliance introduced *Wi-Fi Protected Access (WPA™)* as a strong, standards-based interoperable Wi-Fi security specification. WPA provides assurance to enterprises, small businesses and home users that their data will remain protected and that only authorized users may access their networks. WPA uses Temporal Key Integrity Protocol (TKIP) for data encryption.

In 2004, the Wi-Fi Alliance introduced *Wi-Fi Protected Access 2 (WPA2™),* the second generation of WPA security. Like WPA, WPA2 provides enterprise and home Wi-Fi users with a high level of assurance that their data will remain protected and that only authorized users can access their wireless networks. WPA2 is based on the final IEEE 802.11i amendment to the 802.11 standard ratified in June 2004. WPA2 uses the Advanced Encryption Standard (AES) for data encryption and is eligible for FIPS (Federal Information Processing Standards) 140-2 compliance.

This White Paper is structured to provide a practical hands-on guide for deploying WPA and WPA2 in the enterprise.

Section I provides an overview of Wi-Fi security. It discusses the features and benefits of WPA and WPA2 as over-the-air solutions that bring strong authentication and encryption to the wireless environment. It identifies the components of WPA and WPA2, summarizes how these solutions work to protect wireless networks from attack, and identifies issues that must be addressed before deploying WPA or WPA2 in the enterprise.

Section II identifies the 7 steps to prepare for a WPA or WPA2 Enterprise Deployment. It presents all 7 steps in detail, provides 2 examples of WPA deployment configurations, and reviews WPA and WPA2 deployment configuration tools as well as general WPA and WPA2 deployment guidelines.

Section III discusses transition strategies for a variety of scenarios. These include new Wi-Fi WPA or WPA2 deployments, supporting multiple user communities, upgrading to WPA from vendor proprietary solutions using WEP, and upgrading to WPA or WPA2 from VPN. It also offers a roadmap to future upgrades for organizations that expect to migrate from WPA to WPA2.

If planning a new deployment, managers are advised to read all 3 sections. If planning security upgrades on established Wi-Fi networks, managers should pay specific attention to the passages in Section III that address their particular network scenario.

## SECTION I: Components Overview for WPA and WPA2 Implementations

### Introduction

This section provides a general description and overview of both Wi-Fi Protected Access (WPA), launched in October 2003, and the next generation of Wi-Fi security, Wi-Fi Protected Access 2 (WPA2), launched in September 2004. It describes their features and benefits, identifies the differences between Enterprise and Personal Wi-Fi CERTIFIED™ products, and explains how WPA and WPA2 provide protection from network attacks. Special attention is given to the components needed to build a wireless environment in the enterprise. This section also discusses transitioning enterprises from WPA to WPA2.

WPA and WPA2 are not automatically enabled in the default configuration of new wireless access points (APs) and client devices. They must be configured when the products are installed.

### WPA Features and Benefits

WPA addresses all known vulnerabilities in WEP, the original, less secure 40 or 104-bit encryption scheme in the IEEE 802.11 standard. WPA also provides user authentication, since WEP lacks any means of authentication. Designed to secure present and future versions of IEEE 802.11 devices, WPA is a subset of the IEEE 802.11i specification.

WPA replaces WEP with a strong new encryption technology called Temporal Key Integrity Protocol (TKIP) with Message Integrity Check (MIC). It also provides a scheme of mutual authentication using either IEEE 802.1X/Extensible Authentication Protocol (EAP) authentication or pre-shared key (PSK) technology.

WPA was designed and has been scrutinized by well-known cryptographers. It can be implemented immediately and inexpensively as a software or firmware upgrade to most existing Wi-Fi CERTIFIED™ access points and client devices with minimal degradation in network performance. WPA offers standards-based, Wi-Fi CERTIFIED security. It assures users that the Wi-Fi CERTIFIED devices they buy will be cross-vendor compatible.

When properly installed, WPA provides a high level of assurance to enterprises, small businesses and home users that data will remain protected and that only authorized users may access their networks. For enterprises that have already deployed IEEE 802.1X authentication, WPA offers the advantage of leveraging existing authentication databases and infrastructure.

### WPA2 Features and Benefits

Launched in September 2004 by the Wi-Fi Alliance, WPA2 is the certified interoperable version of the full IEEE 802.11i specification which was ratified in June 2004. Like WPA, WPA2 supports IEEE 802.1X/EAP authentication or PSK technology. It also includes a new advanced encryption mechanism using the Counter-Mode/CBC-MAC Protocol (CCMP) called the Advanced Encryption Standard (AES).

AES satisfies U.S. government security requirements. It has been adopted as an official government standard by the U.S. Department of Commerce and the National Institute of Standards and Technology (NIST). Organizations that require the AES encryption available in WPA2 should be aware that upgrading to it may require new hardware.

Section II of this document offers a roadmap for organizations planning to upgrade to WPA2. Considerations for its deployment are outlined in Section III.

### Enterprise and Personal Modes for WPA and WPA2

There are 2 modes of WPA and WPA2 certification—Enterprise and Personal (See Table 1.1). Both provide an authentication and encryption solution. All Wi-Fi CERTIFIED devices are certified as WPA-Personal by default. Vendors can request additional WPA2-Personal, WPA-Enterprise or WPA2-Enterprise certification. Managers should ask their vendor which certification their devices have, or visit the Wi-Fi Alliance web site, http://www.wi-fi.org to review a list of vendors with WPA-Personal, WPA2-Personal, WPA-Enterprise and WPA2-Enterprise Wi-Fi CERTIFIED products.

Table 1.1 WPA and WPA2 Mode Types

| | WPA | WPA2 |
|---|---|---|
| **Enterprise Mode (Business and Government)** | Authentication: IEEE 802.1X/EAP<br>Encryption: TKIP/MIC | Authentication: IEEE 802.1X/EAP<br>Encryption: AES-CCMP |
| **Personal Mode (SOHO/personal)** | Authentication: PSK<br>Encryption: TKIP/MIC | Authentication: PSK<br>Encryption: AES-CCMP |

### WPA and WPA2 Enterprise Mode

This whitepaper addresses Enterprise Mode deployments. Enterprise Mode operates in a managed mode to meet the rigorous requirements of enterprise security. It leverages the IEEE 802.1X authentication framework which uses an Extensible Authentication Protocol (EAP) type with an authentication server to provide strong mutual authentication between the client and authentication server via the access point.

In this mode, each user is assigned a unique key mechanism for access to the WLAN. This affords a high level of individual privacy. For WPA, TKIP encryption is used. TKIP employs an encryption cipher that issues encryption keys for each data packet communicated in each session of each user, making the encryption code extremely difficult to break. For WPA2, AES encryption is used. AES is stronger than TKIP, thus providing additional network protection.

### WPA and WPA2 Personal Mode

Personal Mode is designed for home and small office/home office (SOHO) users who do not have authentication servers available. It operates in an unmanaged mode that uses a pre-shared key (PSK) for authentication instead of IEEE 802.1X. This mode uses applied authentication in which a pass-phrase (the PSK) is manually entered on the access point to generate the encryption key. Consequently, it does not scale well in the enterprise. The PSK is typically shared among users. A PSK of sufficient strength—one that uses a mix of letters, numbers and non-alphanumeric characters—is recommended.

Personal Mode uses the same encryption methods as Enterprise Mode. It supports per-user, per-session, per-packet encryption via TKIP with WPA or AES with WPA2. Deployments of Personal Mode are not addressed in this whitepaper. Home and SOHO users should consult a vendor to learn more about deploying WPA-Personal or WPA2-Personal and PSK for their environments.

**Protection from Network Attacks with WPA and WPA2**

Both WPA and WPA2 protect the wireless network from a variety of threats, including lost or stolen devices and hacker attacks such as 'man-in-the-middle', authentication forging, replay, key collision, weak keys, packet forging, and 'brute-force/dictionary' attacks.

WPA addresses the weaknesses of original WEP security resulting from WEP's imperfect encryption key implementation and its lack of authentication. Using TKIP, it brings an enhanced encryption algorithm and with IEEE 802.1X/EAP authentication it brings standards-based mutual authentication to Wi-Fi networks. Together, TKIP encryption and mutual authentication insulate the Wi-Fi network from a variety of threats when WPA-Enterprise mode is used.

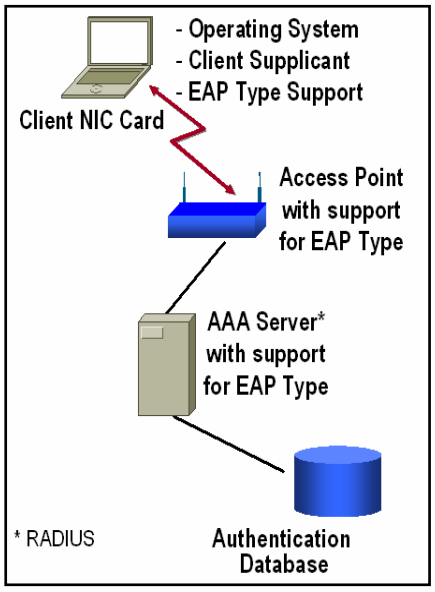
WPA2 offers advanced protection from wireless network attacks. Using AES, government grade encryption and IEEE 802.1X/EAP authentication WPA2 provides stronger standards-based mutual authentication and advanced encryption to protect the Wi-Fi network from a variety of threats and attacks.

**Enterprise Mode Components for a Secure Environment**

Enterprise authentication authorizes users' access to the network on a per-user basis. An authentication deployment confirms user identity and determines the rights for each user.

There are 6 components to authentication in an enterprise deployment for either WPA or WPA2. (See Figure 1.1.) They include:

Figure 1.1 WPA and WPA2 Components




- Client devices that are WPA-Enterprise or WPA2-Enterprise Wi-Fi CERTIFIED
- Client supplicant
- EAP type
- APs that are WPA-Enterprise or WPA2-Enterprise Wi-Fi CERTIFIED
- Authentication server
- Authentication database

All of these components are required. The individual components are discussed below.

***Client Adapter (NIC)***

Client workstations will require the installation of new WPA-Enterprise or WPA2-Enterprise Wi-Fi CERTIFIED client devices or software/hardware upgrades to the presently installed Wi-Fi CERTIFIED devices.

As new equipment is added to the Wi-Fi network, new devices should be WPA-Enterprise or WPA2-Enterprise Wi-Fi CERTIFIED as applicable. In many cases with Wi-Fi CERTIFIED products, only a software or firmware upgrade is needed for WPA; new hardware is not required. For WPA2, a hardware upgrade may be required. Managers should ask their vendor what is required to upgrade a client adapter to WPA or WPA2. (When using a proprietary solution or WEP that cannot be upgraded, managers should see Section III—Deployment Scenarios).

### *Client Supplicant*

An IEEE 802.1X supplicant is required on the client. A supplicant is software that is installed on the client to implement the IEEE 802.1X protocol framework and one or more EAP methods. When deploying WPA or WPA2, managers should make sure that all client devices possess the necessary supplicant for their operating system. If a supplicant is not present, network managers must obtain one.

Supplicants may be included in the client operating system, integrated into drivers, or installed as third-party standalone software. Some vendors of wireless client devices ship the supplicant with their cards. Wi-Fi CERTIFIED client devices are confirmed to work with Microsoft, Funk Software, or a vendor supplied WPA or WPA2-enabled supplicant. However, the device need not possess the supplicant to be WPA-Enterprise or WPA2-Enterprise Wi-Fi CERTIFIED. Network managers should check with their vendor to confirm if supplicants are included with the client devices.

### *EAP Authentication Types*

Extensible Authentication Protocol (EAP) types offer a range of options that can be used with different authentication mechanisms, operating systems, and back-end databases. Each maps to different types of user logins, credentials and databases used in authentication. The EAP type used in a WPA-Enterprise or WPA2-Enterprise deployments should be selected to support the organization's security strategy in accordance with the client supplicants and the back-end database used to store client identity credentials. (See Selecting an EAP Type).

The Wi-Fi Alliance certifies WPA-Enterprise and WPA2-Enterprise products in tests on an open architecture in which EAP-TLS is used. However, as WPA and WPA2 are open platforms that are designed to be extensible, other EAP types that are not tested by the WPA or WPA2 certification program should run in a WPA or WPA2 environment. Example EAP types include EAP-TLS, EAP-TTLS, PEAP v.0, PEAP v.1 and other open standard types. The Wi-Fi Alliance plans to add more EAP types to its interoperability testing in the future. Managers should ask their vendor about other EAP types.

### *Access Points*

New APs to be deployed in an enterprise network using EAP authentication should be WPA-Enterprise or WPA2-Enterprise Wi-Fi CERTIFIED. Currently installed Wi-Fi CERTIFIED APs may be upgradeable to WPA-Enterprise or WPA2-Enterprise via a firmware or hardware upgrade; otherwise a new AP will be required. (If there is hardware running WEP or a proprietary solution that cannot be upgraded, see Section III—Deployment Scenarios).

### *Authentication Server/Database*

WPA-Enterprise and WPA2-Enterprise employs IEEE 802.1X authentication with EAP types which provide mutual authentication on Wi-Fi networks. This helps to insure that only authorized users are granted access to the network and that users only access authorized areas within the network. The requirements for an authentication server in a wireless network are similar to those of a wired LAN; the authentication server stores the list of the names and credentials of authorized users against which the server verifies user authenticity. Typically, a Remote Authentication Dial-In User Service (RADIUS) server is used.

User credentials may also be stored in an external database, such as SQL, LDAP or Active Directory, that can be accessed by the authentication server. The configuration is not determined by standards and can be specific to implementation.

Organizations that have already deployed a proprietary solution with WEP and an authentication server will have these basic components in place. If these devices are Wi-Fi CERTIFIED™, only upgrades to WPA-Enterprise or WPA2-Enterprise for the APs and client devices should be required. Once deployed, new authentication protocols can usually be implemented without

changes to the infrastructure. If an authentication infrastructure has already been deployed for the wired LAN, it may be utilized for WPA or WPA2. Managers should heck with their vendor about transitioning an existing 802.1X deployment to WPA or WPA2.

## WLAN Authentication and Encryption Methods

### *Static WEP and Dynamic WEP with IEEE 802.1X*

WEP is the original, static 40-bit or 104-bit encryption scheme in the IEEE 802.11 standard. It lacks any means of authentication. WEP has been proven to be insecure and vulnerable to network attacks.

WEP with IEEE 802.1X, is referred to as “dynamic WEP”. Dynamic WEP is a non-standard interim technology that some vendors introduced after the weaknesses of static WEP were uncovered. It uses WEP encryption with IEEE 802.1X authentication. Because it still uses WEP encryption, dynamic WEP deployments are also insecure and vulnerable to network attacks.

The Wi-Fi Alliance does not recommend deploying a Wi-Fi network with static WEP or dynamic WEP. Both methods are insecure and should be transitioned to WPA or WPA2.

### *How WPA and WPA2 Authentication Works*

WPA-Enterprise and WPA2-Enterprise mutual authentication is initiated when a user associates with an access point. The AP blocks access to the network until the user can be authenticated. The user provides credentials which are communicated to the authentication server. The authentication process is enabled by the IEEE 802.1X/EAP framework. With EAP, IEEE 802.1X creates a framework in which client workstations and the authentication server mutually authenticate with one another via the AP. Mutual authentication helps to ensure that only authorized users access the network and confirms that the client is authenticating to an authorized server. It helps to protect users from accidentally connecting to unauthorized ‘rogue’ APs.

If the authentication server accepts the user’s credentials, the client joins the WLAN. If not, the client remains blocked. Once the user has been authenticated, the authentication server and the client simultaneously generate a Pairwise Master Key (PMK).

A 4-way handshake then takes place between the client and the AP, to complete the process of authenticating the AP with the client, establishing and installing the TKIP (WPA) or AES (WPA2) encryption keys. As the client begins communicating on the LAN, encryption protects the data exchanged between the client and the AP.

### *How WPA Encryption with TKIP Works*

WPA addresses the weaknesses of WEP with the strong dynamic encryption provided by TKIP. TKIP encryption replaces WEP’s small (40-bit) static encryption key, manually entered on wireless APs and client devices, with a 128 bit per-packet key. WPA uses a methodology that dynamically generates keys and removes the predictability that intruders rely upon to exploit the WEP key. WPA also includes a Message Integrity Check (MIC), designed to prevent an attacker from capturing, altering and resending data packets. WPA operates at the Media Access Control (MAC) layer.

In this process, after accepting a user’s credentials, the authentication server uses 802.1X to produce a unique master, or ‘pair-wise’, key for that user session. TKIP distributes the key to the client and AP, setting up a key hierarchy and management system. TKIP dynamically generates unique keys to encrypt every data packet that is wirelessly communicated during a session. This

hierarchy replaces WEP's single static key with some 280 trillion possible keys that can be generated for a given data packet.

The MIC is employed to prevent an attacker from capturing, altering and resending data packets. The MIC provides a strong mathematical function in which the receiver and the transmitter each compute and then compare the MIC. If it does not match, the data is assumed to have been tampered with and the packet is dropped—unless the optional MIC countermeasure is implemented in which case all clients are deauthenticated and new associations are prevented for one minute.

### *How WPA2 Encryption with AES Works*

AES is a block cipher, a type of symmetric key cipher that uses groups of bits of a fixed length - called blocks. A symmetric key cipher is a cipher that uses the same key for both encryption and decryption. The word cipher is used in cryptography to describe the instructions or algorithm used for encrypting and decrypting information.

With AES, bits are encrypted in blocks of plaintext that are calculated independently, rather than a key stream acting across a plaintext data input stream. AES has a block size of 128 bits with 3 possible key lengths 128, 192 and 256 bits as specified in the AES standard. For the WPA2/802.11i implementation of AES, a 128 bit key length is used. AES encryption includes 4 stages that make up one round. Each round is then iterated 10, 12 or 14 times depending upon the bit-key size. For the WPA2/802.11i implementation of AES, each round is iterated 10 times.

AES uses the Counter-Mode/CBC-Mac Protocol (CCMP). CCM is a new mode of operation for a block cipher that enables a single key to be used for both encryption and authentication. The 2 underlying modes employed in CCM include Counter mode (CTR) that achieves data encryption and Cipher Block Chaining Message Authentication Code (CBC-MAC) to provide data integrity.

CBC-MAC is used to generate an authentication component as a result of the encryption process. This is different from prior MIC implementations, in which a separate algorithm for integrity check is required. To further enhance its advanced encryption capabilities, AES uses a 48-bit Initialization Vector (IV). AES has no known attacks and the current analysis indicates that it takes $2^{120}$ operations to break an AES key—making it an extremely secure cryptographic algorithm.

### *WPA and WPA2 Security Advantage*

When compared with the IEEE 802.11 security standard using 40-bit WEP with no dynamic keying, TKIP and AES make it far more difficult-if not impossible-for a would-be intruder to break into a Wi-Fi network. By greatly expanding the size of keys and number of keys in use, creating an integrity checking mechanism, using a strong encryption cipher; and imposing replay protection, AES and TKIP greatly increase the strength and complexity of wireless encryption. Together with the IEEE 802.1X/EAP mutual authentication framework, TKIP and AES magnify the complexity and difficulty involved in decoding data on a Wi-Fi network—making the Wi-Fi network secure.

## Understand Your Security Environment

In most enterprise settings, Wi-Fi security will be a part of an overall network security strategy that addresses both the wired and wireless segments of the network. The IEEE 802.1X framework can support both wired and wireless security within the enterprise network. Wi-Fi security policies must, therefore, fit into the security environment for the entire enterprise. As in a wired network, a good security policy in a wireless environment should address the means by

which users prove their identities, the means by which access is controlled after they are authenticated, and the means in which user identity information is stored.

### *How Do Users Prove Their Identity?*

Users make a claim of identity by presenting credentials in the form of passwords, certificates, tokens, biometrics, or other means. Each method offers advantages and disadvantages. The method of identity that is selected is determined by manager preferences relative to level of technology deployed, credentialing rigor, and management of credentials. The more advanced and rigorous the technology, the more difficult it is for an intruder to forge an identity and gain access to the network. However, the management of those credentials may also increase complexity.

For example, a biometric system of identity using a fingerprint or eye scan is the most difficult to forge but it presents management challenges in large enterprises. One-time tokens, used with a pass-phrase that leverages a shared key for log-in, plus a constantly changing password on the token, may be more realistic in large enterprises. If the token is lost or stolen, an intruder who recovers it would be unable to access the network without also knowing the code. Identities that are easiest to forge are those that rely on devices that can be lost or stolen. For example, a system which employs MAC address authentication on a wireless network interface card (NIC) without also requiring a password or pass-phrase is susceptible to anyone who recovers a lost or stolen card.

### *How Is User Access Controlled After Authentication?*

A good security policy must also address what users may access after their claim of identity has been accepted. It should consider the network infrastructure, as well as issues such as how users get to the server, what they see when they get there, traffic priority and bandwidth management.

Because user access to applications and data is determined at a higher layer than Layer 2 protection for wired or wireless networks, it is not addressed in this whitepaper. However, managers should address it in best practices to an overall security policy, as standard network security practices will apply once a user is authenticated on the network.

### *How Is User Identity Information Stored?*

In the context of WPA and WPA2, the issues that need to be addressed when defining a data storage strategy are the location of user identity credential storage and choice of database, if an external one is chosen. This data storage decision will impact choice of an EAP type, which is dependent upon the type of identity database that is used and any special activities intended for support. One example of a special activity would be Subscriber Identity Module (SIM)-based roaming, which allows mobile users to associate with new APs without having to log in again. If not storing user identity credentials on the Authentication server, then managers can use SQL, Active Directory, or Novell's LDAP.

### *Selecting an EAP Type*

EAP types that are supported by IEEE 802.1X include EAP-TLS, EAP-TTLS, PEAP v.0, PEAP v.1, and other open standard types. Various EAP types map to different supplicants and login types. Each is designed to solve different problems. Each offers different sets of advantages and disadvantages within a security environment. They also entail different overhead. Some are best suited in environments where access is controlled by simple passwords; others are designed to support client and/or server-side certificates. EAP methods which support mutual authentication must be used in WLAN environments.

The Wi-Fi Alliance certifies WPA-Enterprise and WPA2-Enterprise products in tests on an open architecture in which EAP-TLS is used. Expansion of the WPA-Enterprise and WPA2-Enterprise

certification programs is planned with testing of additional EAP types. Since WPA and WPA2 are open platforms, designed to be extensible, other EAP types should run in a WPA-Enterprise or WPA2-Enterprise environment, allowing a variety of authentication protocols to be implemented without changes to the infrastructure when authentication is deployed.

The EAP type installed will depend upon the network environment and the security policies put in place. Managers may also choose to deploy more than one EAP type, depending upon the needs of the various user communities supported. (See Section III—User Communities with Multiple Credentials, Multiple Databases and Different EAP Types).

Figure 1.2 contrasts the features of 3 common EAP types, PEAP, EAP-TLS and EAP-TTLS to illustrate the security environments to which they are best adapted. The features listed at the left of the chart are issues to consider when comparing EAP types. Managers should ask their vendor about how other EAP types compare.

Figure 1.2 EAP Authentication Type Comparison

| | PEAP | EAP-TLS | EAP-TTLS |
|---|---|---|---|
| **User Authentication Database and Server** | OTP, LDAP, NDS, NT Domains, Active Directory | LDAP, NT Domains, Active Directory | OTP, LDAP, NDS, NT Domains, Active Director |
| **Native Operating System Support**[1] | Windows XP, 2000 | Windows XP, 2000 | Windows XP, 2000, ME, 98, WinCE, Pocket PC2000, Mobile 2003 |
| **User Authentication Method** | Password or OTP[2][3] | Digital Certificate | Password or OTP[4] |
| **Authentication Transaction Overhead** | Moderate | Substantial | Moderate |
| **Management Deployment Complexity** | Moderate Digital Certificate For Server | Substantial Digital Certificate Per Client and For Server | Moderate Digital Certificate For Server |
| **Single Sign On** | Yes[5] | Yes | Yes |

### Transitioning from WPA to WPA2

As explained earlier, the IEEE 802.1X/EAP authentication framework is used in both WPA and WPA2. Enterprises deploying WPA-Enterprise today should consider the ability to upgrade their network to WPA2-Enterprise in the future. Existing WPA equipment may require a software or hardware upgrade to support WPA2. When transitioning from WPA to WPA2, some WPA equipment may not be upgradeable because of AES encryption processing requirements.

---

[1] Other operating systems can be supported with supplicants
[2] OTP and Token are types of 2-Factor authentication
[3] Requires a server side certificate
[4] OTP and Token are types of 2-Factor authentication
[5] Microsoft PEAP (EAP-MSCHAPv2) affords single sign on for Windows. Other supplicants may afford other single sign on login mechanisms

Managers should check with their vendor about the best process to transition from WPA to WPA2.

**Summary**

WPA and WPA2 fix all known vulnerabilities in WEP and greatly enhance data protection and access control on existing and future Wi-Fi LANs. They provide an immediate, strong, standards-based, interoperable Wi-Fi security solution.

Before proceeding with a WPA or WPA2 deployment, a manager should have a good understanding of the security policies it will support. Mangers should read Part II and Part III of this document in which we present 7 steps to prepare for WPA and WPA2 deployment and describe various deployment scenarios.

## SECTION II—Steps and Tools for WPA and WPA2 Deployment

### Introduction

The migration path in upgrading to WPA or WPA2 will depend upon the security environment and the user authentication policies in place. In this section, we present the 7 Steps to Prepare for a WPA or WPA2 Deployment. These steps focus on the authentication portion of WPA and WPA2. This section also reviews 2 common configurations and presents several WPA and WPA2 deployment tools.

### 7 Steps to Prepare for WPA or WPA2 Deployment

Each of the 7 steps listed below is required to determine the components of a WPA or WPA2 deployment. They will prepare network managers to deploy WPA or WPA2 including the implementation of IEEE 802.1X authentication and TKIP (WPA) or AES (WPA2) encryption for an enterprise environment.

After following all 7 steps, managers will know the components needed for a WPA or WPA2 deployment and be prepared to implement IEEE 802.1X authentication policies and begin deployment. Enterprises that already have an IEEE 802.1X/EAP framework for wireless computing in place and intend to continue using it will have already addressed the first 6 steps and may begin at step 7.

These 7 steps address the requirements for any network using IEEE 802.1X authentication. The effort and investment made in following the 7 steps will serve for both WPA and WPA2 deployments. Whether deploying WPA-Enterprise or WPA2-Enterprise, managers *must* address all 7 steps.

The 7 steps are:

- Step 1: Security Mechanism and Credentials
- Step 2: User Authentication Database
- Step 3: Client Operating Systems
- Step 4: Supplicants
- Step 5: EAP Types
- Step 6: Authentication Server
- Step 7: Access Points and Client NIC Cards

#### *Step 1—Security Mechanism and Credentials*

Many existing enterprise networks already have a network security policy in place. Security policies, credentials and user identity management mechanisms will impact WPA and WPA2 enterprise deployment. Typically, the database is stored on the server or, externally, in Microsoft Active Directory™, Novell LDAP™, iPlanet™ or Secure ID™ Token.

If already running IEEE 802.1X authentication, and an authentication system is in place, a manager can continue to use it to store security credentials if it supports the EAP type(s) selected for the Wi-Fi network.

If there is not already a security policy in place, a manager will have to select one, provide the necessary user credentials to support it, and confirm that the credentials chosen can be managed by the authentication server. (See Section I, How Do Users Prove Their Identity?)

***Step 2—User Authentication Database***

A database is required for user authentication. If users are already being authenticated, managers should consider the database already in house. In the absence of an existing user authentication database, managers will have to select one.

Selection should be based on the following considerations:

- The security policy and the management of user credentials
- The credential type selected
- How user identity information will be stored
- Budget considerations
- Server environment

The server environment (UNIX, Linux, or NT) will heavily influence what database is implemented. Managers should consult their vendor.

***Step 3—Client Operating Systems***

Determine which client operating systems (OS) will be supported — Windows XP, 2000, NT, 98, 95; Windows CE; Mac OS; Linux; Palm OS; DOS or a proprietary system. Managers should make sure that EAP type, selected database, and supplicants will support the operating system that will be used with WPA or WPA2.

***Step 4—Supplicants***

This step and Step 3 (Client Operating Systems), Step 5 (EAP Types), and Step 6 (Authentication Server) should be considered in parallel as the selection of the supplicant should be based on the EAP types, as well as on the client operating systems and authentication database being used.

Managers should determine if they already have a supplicant to support existing client operating systems. If not, one should be obtained. Some operating systems include free supplicants. Others require the purchase of an after-market supplicant. In some settings, aftermarket supplicants may offer more flexibility as they are not tied to a particular operating system. Features may vary between built-in supplicants and third party supplicants.

***Step 5—EAP Types***

In parallel with Step 4, decide which EAP-type will be used. The EAP type selected should support the selected database for user credentials and the network security strategy. It should match the user authentication policies, user management strategy, and client operating system. (See Section I, Selecting an EAP Type).

Some examples of EAP types that match various databases include:

- Microsoft format NT or Active Directory—works with PEAP v0/-MSCHAP v2, EAP-TLS, and EAP-TTLS/ MSCHAP v2
- LDAP or Netscape Directory Service (NDS)—works with PEAP v1/ MD5, PEAP v1/ GTC, EAP-TLS, EAP-TTLS/CHAP
- A token or one-time password (OTP) server—The server has a token card with a reference ID that works with PEAP v1/EAP-GTC, EAP-TTLS/GTC

Managers should ask their vendor how other EAP types compare. Since the Wi-Fi Alliance certifies WPA-Enterprise and WPA2-Enterprise products in tests on an open architecture, a variety of open standard and other EAP types can be used. Additional information about EAP types is included in Section I of this whitepaper.

***Step 6: Authentication Server***

Select an authentication server that will work with the selected user credentials database and matching EAP types. Managers may change EAP types to match the current server. Or, managers may wish to purchase a new server to work with the EAP type that best supports their security policies. Typically, a RADIUS server is used. If selecting a new server, managers must verify that it will work with the selected database and matching EAP-types.

***Step 7: Access Points and Client NIC Cards***

Confirm that all APs and client devices to be used in the deployment are WPA-Enterprise or WPA2-Enterprise Wi-Fi CERTIFIED as applicable. WPA-Personal and WPA2-Personal APs and clients are not recommended for enterprise deployments because they do not support IEEE 802.1X and EAP authentication. (See discussion of WPA and WPA2 Personal Mode in Section I).

Typically, WPA and WPA2 are not automatically implemented in the default configuration of new wireless client devices and APs. They must be configured when the products are installed.

Legacy devices may require WPA or WPA2 upgrades. Many vendors provide WPA firmware updates for legacy APs and client devices. A hardware upgrade may be needed for WPA2 devices. Managers should contact their vendor for upgrade information regarding the devices already in place. A list of product vendors with products that are WPA-Enterprise and WPA2-Enterprise Wi-Fi CERTIFIED is available at www.wi-fi.org.

## 2 Examples of WPA Deployment Configurations

The 2 examples of WPA-Enterprise deployment configurations shown below illustrate how the 7 Steps to Prepare for WPA or WPA2 Deployments might apply in a Windows environment and in a Macintosh environment. Manager should work with their vendor to determine the correct WPA or WPA2 deployment configuration for their Wi-Fi network. Each WPA-Enterprise example below uses TKIP encryption.

***Example 1—Windows***

1. Security Credentials: Digital Certificate X.509
2. Database: Microsoft Active Directory
3. Client OS: Windows XP
4. Supplicant: Built into Windows XP for EAP-TLS
5. Authentication EAP Type: EAP-TLS
6. Authentication Server: Cisco Secure Access Control Server (RADIUS server)
7. Access Points and Client Devices: WPA-Enterprise Wi-Fi CERTIFIED

***Example 2—Macintosh***

1. Security Credentials: Password and one-time password (OTP, an RSA secure ID token)
2. Database: LDAP/Netscape directory service
3. Client OS: Macintosh OS 10.2
4. Supplicant: Mac OS 10 includes EAP-TTLS/MSCHAPv2
5. Authentication EAP-Type: Mac with EAP-TTLS/MSCHAPv2
6. Authentication Server: Funk Steel-Belted RADIUS™
7. Access Points and Client Devices: WPA-Enterprise Wi-Fi CERTIFIED

**WPA and WPA2 Deployment Configuration Tools**

The Wi-Fi Alliance recommends an assigned Cut-Over Day to transition directly to WPA or WPA2. To transition from WPA to WPA2, the Wi-Fi Alliance recommends using the Mixed Mode available in WPA2. Both of these options are reviewed below.

This paper also includes 2 additional vendor proprietary deployment tools that a vendor may suggest to transition to WPA from WEP. These are Multiple Wi-Fi Network and Vendor Proprietary Transition Mode. The Wi-Fi Alliance does not recommend these tools. However, they are presented here to assist managers with understanding how they may impact their WPA or WPA2 deployment.

Managers should work with their vendor to select the deployment method that works best in their environment.

***Assigned Cut-Over Day***

Managers may establish a specified day and time when all users must switch to WPA or WPA2. The cut-over can be implemented in one day or across multiple days. Following the cut-over, the previous encryption type or wireless solution should not be available to users. This will assure that all users are using only the WPA-Enterprise or WPA2-Enterprise solution.

This solution takes coordination among the IT department and employees and requires that all components of the WLAN network be upgraded to WPA or WPA2 prior to the cut-over day.

***Multiple Wi-Fi Network***

Some vendors may suggest using Multiple Wi-Fi Networks to support legacy WEP devices that cannot transition to WPA. This option is not secure. It is not recommended by the Wi-Fi Alliance. It is presented here to assist companies that may need to address this situation.

A Multiple Wi-Fi Network is intended to be a *temporary, transitional solution only* and should not be used as a long term solution for legacy WEP devices that cannot be transitioned to WPA.

Multiple Wi-Fi networks use multiple Service Set Identifiers (SSIDs) to support separate authentication strategies or encryption policies. Multiple Wi-Fi networks may be recommended by a vendor as a *short-term* solution for deployment from an existing Wi-Fi network to WPA until all devices can be transitioned to a more secure solution.

In deploying a Multiple Wi-Fi Network, one of the following 2 options would be used:

- Option 1: Overlay Configuration: An overlay configuration in which 2 or more WLANs are deployed in the same area simultaneously. Use multiple access points with each supporting one SSID and security policy. Any Wi-Fi access point can be used in an overlay configuration. This option requires additional channel and traffic planning.

- Option 2: Vendor Proprietary Solution: Some vendors offer a vendor proprietary solution where each access point supports multiple SSIDs simultaneously. Managers should check with their vendor to see if this is available.

***Vendor Proprietary Transition Mode***

Some vendors offer a proprietary WEP-to-WPA transition mode built into their enterprise access points to permit the coexistence of WPA and legacy WEP clients on a common SSID.

Vendor Proprietary Transition Mode allows large enterprises to upgrade gradually to WPA, supporting the use of WPA alongside WEP while the network is in transition. Like Multiple Wi-Fi

networks, this mode is not secure. This solution is not recommended by the Wi-Fi Alliance. It is explained here to assist companies who may need to address this situation.

Vendor Proprietary Transition Mode is intended to be a *temporary, transitional solution only* and should not be used as a long term solution for legacy WEP devices that cannot be transitioned to WPA.

Vendor Proprietary Transition Mode is applied at the access point. During its operation, the access point advertises which encryption ciphers (e.g. WEP, TKIP) are available. The client device selects the encryption cipher to be used. Once selected, that cipher is used to encrypt communication between the client and access point.

Since all clients must be able to decode the broadcast packets, Vendor Proprietary Transition Mode operation presents the added disadvantage of using WEP to encrypt all broadcast packets. Best security practices dictate that a network is only as secure as its weakest link which, when Vendor Proprietary Transition Mode is used, is WEP. For that reason, WEP-keyed users leave the network vulnerable to WEP key attacks. WPA users will not receive the full benefits of WPA until the transition is complete and WEP is disabled.

If a manager intends to use Vendor Proprietary Transition Mode during a transition to WPA, check with the vendor to confirm that it is supported on the APs. Vendor Proprietary Transition Mode is disallowed by Wi-Fi certification and is not present in all APs. VPN or other supplementary security should be enabled for clients who use WEP during this time period to insure security across the network.

### *WPA2 Mixed Mode*

WPA2 includes an optional mixed mode operation (WPA2 Mixed Mode) that permits the coexistence of WPA and WPA2 clients on a common SSID. WPA2 Mixed Mode is a Wi-Fi Alliance supported feature. This mode can be used during the transition from WPA to WPA2. In WPA2 Mixed Mode, the access points advertise which unicast encryption ciphers (TKIP or CCMP) are available for use and the client selects the one it would like to use. TKIP is always advertised as the broadcast/multicast traffic cipher because the goal of WPA2 Mixed Mode is to help transition older equipment. Therefore, the weakest broadcast/multicast cipher, TKIP, is advertised in a WPA2 Mixed Mode environment. Unlike WEP to WPA mixed mode, WPA to WPA2 mixed mode is a secure operating mode.

With WPA2 Mixed Mode, once the client selects the cipher, that cipher is used to encrypt all unicast communications between the client and access point. This option provides enterprise-class security because it supports encryption with either TKIP or AES. Managers should check with their vendor to see if this is available.

## General WPA and WPA2 Deployment Guidelines

In deploying WPA-Enterprise or WPA2-Enterprise on any new or existing WLAN network, managers must implement APs with an authentication server that is configured to support WPA or WPA2. The IT department must schedule the transition for each component. The order in which the components are deployed will impact the WPA or WPA2 transition.

During the deployment process, a selected transition mode may be used to facilitate the upgrade. However, as long as any part of the network continues to run WEP, additional security mechanisms, such as VPN, should remain in place to ensure security. If Vendor Proprietary Transition Mode is used, it should be turned off when the entire network has been upgraded to WPA (i.e. all APs and WEP clients have been upgraded to WPA or WPA2).

Some WEP devices cannot be upgraded to WPA or WPA2. In these cases, a decision must be made to either replace those clients with devices that support WPA or WPA2 or make accommodations to separate the less secure WEP clients from the secure WPA and WPA2 clients—with the understanding that any clients running WEP pose a network security risk. The Wi-Fi Alliance does not recommend supporting any clients that do not run WPA or WPA2.

**Summary**

The general deployment guidelines in this section, including the 7 Steps to Prepare for WPA and WPA2 Deployment, apply to any new WPA deployment, as well as upgrades to WPA on existing Wi-Fi networks. The 7 Steps include: security mechanisms and credentials, user authentication database, client operating systems, supplicants, EAP types, authentication server, and access points and client NIC cards.

If an authentication server has not already been deployed, managers will need to follow each step outlined in this section to complete the WPA and WPA2 deployments. Managers should understand the security environment and user authentication policies to select the EAP authentication types that best fit their needs.

If an existing Wi-Fi network includes WEP devices that cannot be upgraded to WPA or WPA2, the Wi-Fi Alliance recommends replacing these devices with new WPA-Enterprise or WPA2-Enterprise Wi-Fi CERTIFIED devices. Mixed WEP to WPA operating modes, such as Multiple Wi-Fi Networks or Vendor Proprietary Transition Mode are insecure and as such are not recommended by the Wi-Fi Alliance. However, companies may choose one of these options based on their vendor's recommendation. Both options should be used only temporarily to facilitate the WEP to WPA or WPA2 transition process and, during that time, VPN or other security technologies should be used to insure security across the Wi-Fi network.

WPA2 includes a secure WPA2 Mixed Mode, a Wi-Fi Alliance supported option that allows for the secure co-existence of WPA and WPA2 devices on the same network. This mode accommodates gradual, secure transitions from WPA to WPA2.

Managers should next review the deployment scenarios outlined in Section III and follow the one that best describes their planned migration path to WPA or WPA2.

# SECTION III — WPA and WPA2 Deployment Scenarios

## Introduction

This section discusses various deployment scenarios and offers guidelines for deploying new Wi-Fi WPA networks and for upgrading existing Wi-Fi networks to WPA. Additionally, considerations for deployments of WPA2 are given.

The Wi-Fi Alliance recommends that companies deploy WPA or WPA2. Companies can safely deploy WPA or WPA2 today or deploy WPA today and transition to WPA2 at a later date. This section discusses transition strategies for a variety of deployment scenarios, including:

- New Wi-Fi WPA deployments
- Upgrading user communities where multiple credentials, databases and EAP types are required
- Upgrading to WPA or WPA2 from WEP
- Upgrading to WPA or WPA2 from VPN
- Transitioning from WPA to WPA2

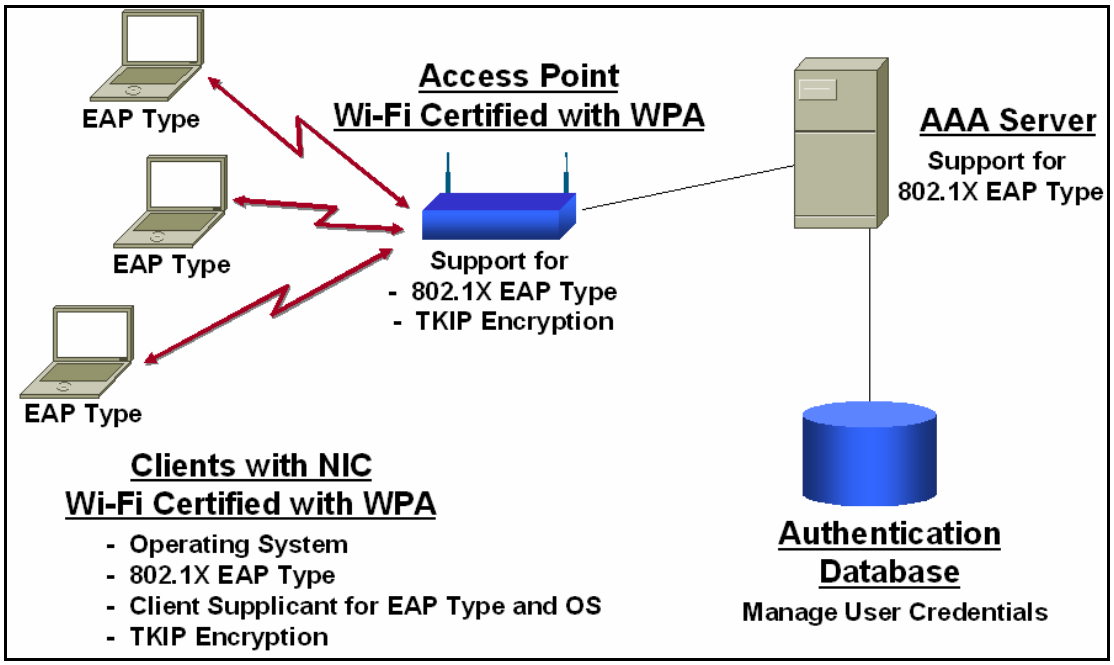
## New Wi-Fi WPA or WPA2 Deployment

If deploying WPA or WPA2 across a new stand-alone wireless network or adding wireless segments to an existing wired network, managers should follow all 7 Steps to Prepare for WPA or WPA2 Deployment, as outlined in Section II.

After selecting WPA-Enterprise or WPA2-Enterprise Wi-Fi CERTIFIED APs and client devices and following all 7 steps, managers will follow the specific installation guidelines for their devices. A sample configuration for a new WPA deployment is illustrated in Figure 3.1. Multiple EAP types can be used to support different user communities and security policies. (See the next section, User Communities with Multiple Credentials, Multiple Databases and Different EAP types).

Figure 3.1 New Wi-Fi Deployment

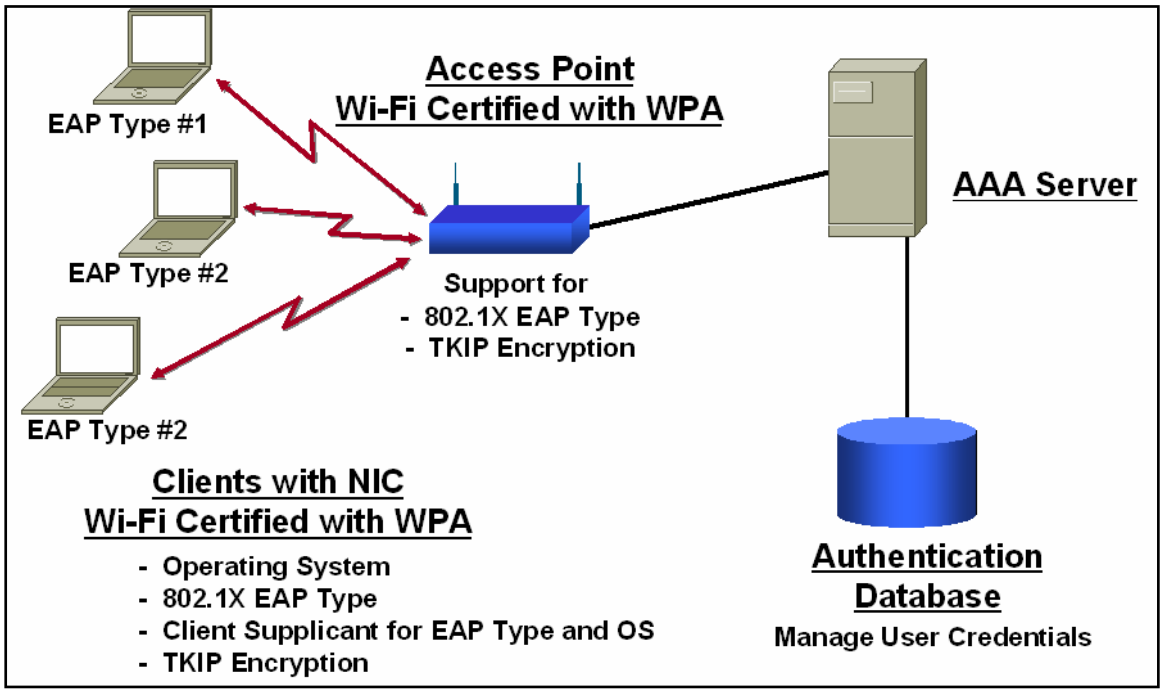



**Upgrading Existing Wi-Fi Network — User Communities with Multiple Credentials, Multiple Databases and Different EAP types**

As in a wired network, multiple EAP types can be used on a Wi-Fi network to support multiple user groups with different security requirements, different credentials, and different operating systems, as illustrated in Figure 3.2.

The security requirements of the various user groups, and the solutions selected to meet them, will affect the EAP type selected for each group. User credentials are managed at the authentication server or the credentials database.

Figure 3.2 Multiple credentials, multiple databases and different EAP types




Here again, the 7 Steps to Prepare for a WPA or WPA2 Deployment apply. The IT department must schedule the transition of each component. Review the steps outlined in the previous section, *WPA and WPA2 Deployment Configuration Tools*.

Managers should evaluate their network and work with their vendor to determine the best plan to facilitate the upgrade and to maintain the integrity of their user groups.

**Upgrading an Existing Wi-Fi Network to WPA — WEP to WPA or WPA2**

If using a proprietary system that includes WEP, the Wi-Fi Alliance advises that managers transition from WEP to WPA or WPA2 as quickly as possible to insure strong security on their Wi-Fi network. WPA or WPA2 are upgrade paths for WEP or other security methods that are less secure than WPA or WPA2.

The migration process to WPA or WPA2 from a proprietary system that includes WEP involves:

- Upgrading installed APs and client devices to WPA or WPA2
- Migrating users from WEP to WPA or WPA2 following the 7 Steps to Prepare for a WPA or WPA2 Deployment

If there are no residual users who cannot migrate to WPA or WPA2 and all WEP devices will be discontinued following the migration, managers can use the Cut-Over Day approach, or temporarily use Vendor Proprietary Transition Mode (if it is supported) or a Multiple Wi-Fi Network to facilitate the migration. Managers should use VPN or other security mechanisms to protect the network during the transition if WEP is used by any client devices. Supplemental security technologies, such as VPN, will not be necessary for the purpose of securing a Wi-Fi network once WPA or WPA2 are deployed.

If there are legacy WEP devices that cannot migrate to WPA or WPA2, the Wi-Fi Alliance recommends that managers purchase new WPA-Enterprise or WPA2-Enterprise Wi-Fi CERTIFIED devices. The Wi-Fi alliance does not recommend deploying or maintaining a Wi-Fi network with WEP.

***Static WEP***

If deploying WPA from static WEP, the WLAN environment is insecure and managers must follow all 7 Steps to Prepare for a WPA or WPA2 Deployment. Some legacy devices are static WEP-only and cannot be upgraded to WPA or WPA2. If there are legacy static WEP devices that cannot be upgraded, it is recommended that managers replace them with WPA-Enterprise or WPA2-Enterprise devices.

***WEP with IEEE 802.1X***

In a dynamic WEP environment, many of the 7 Steps to Prepare for a WPA or WPA2 Deployment outlined at the beginning of Section II may have already been completed to provide the authentication framework currently in use. If dynamic WEP is in place, managers should review the steps, repeating any that may be applicable, and upgrade all APs and NICs (and possibly the client supplicants) to support WPA or WPA2. These steps should be used as guidelines to the transition. Managers should review their transition strategy with their vendor before proceeding.

If all dynamic WEP devices cannot be upgraded to WPA or WPA2, the Wi-Fi Alliance recommends that managers purchase WPA-Enterprise or WPA2-Enterprise Wi-Fi CERTIFIED devices. The Wi-Fi Alliance does not recommend deploying a Wi-Fi network with static WEP or dynamic WEP.

***Common WEP to WPA Transition Questions and Answers***

The following questions provide a decision-matrix to help managers transition from WEP to WPA:

**1. Can you migrate all clients to WPA?**
If yes, move on to question #2 below. It will help you assess how to implement your transition from WEP to WPA.

If no, the Wi-Fi Alliance recommends that you purchase WPA-Enterprise Wi-Fi CERTIFIED devices.

**2. If you can migrate all devices to WPA, do you want to use multiple or single SSIDs during the transition?**
If you opt for multiple SSIDs, move on to question #3 below.

If you choose single SSIDs, your vendor may recommend using Vendor Proprietary Transition Mode during the transition. The Wi-Fi Alliance does not recommend using Vendor Proprietary Transition Mode. This mode is fundamentally insecure. As long as any portion of the network continues to run WEP, other security mechanisms such as VPNs should be in place to secure the Wi-Fi network until the entire network can be upgraded.

**3. Do you want to use multiple SSIDs with a single AP or multiple APs during the transition?**
If you opt to use multiple APs, your vendor may recommend using Multiple Wi-Fi Network Option 1 - Overlay Configuration, as described in Section II.

If you use a single AP, your vendor may recommend using use Multiple Wi-Fi Network Option 2 – Vendor Proprietary Solution, as described in Section II.

**Upgrading an Existing Wi-Fi Network to WPA—VPN to WPA or WPA2**

In environments where VPN technology has been used to secure the WLAN, the APs operate in open mode with no other security in place. Some companies have deployed WEP with VPN encryption to provide clients with a secure connection.

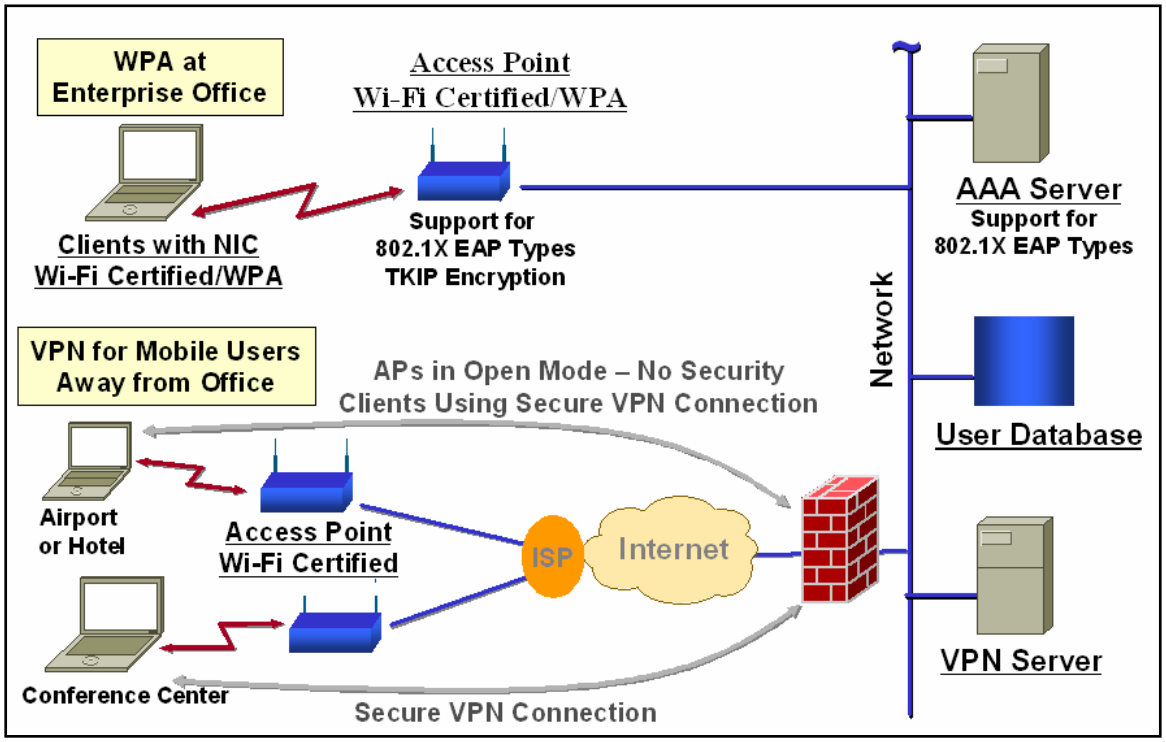
WPA and WPA2 eliminate the need to use VPN technology to secure Wi-Fi networks within the enterprise environment. Once a transition to WPA or WPA2 is complete, VPN is no longer necessary for securing the Wi-Fi network within the enterprise. VPNs, however, may continue to be used to secure the connections of mobile users accessing the enterprise network via dial-up and other remote connections, including connections made through public access WLANs (hot spots). See Figure 3.3.

The WPA or WPA2 upgrade process on a Wi-Fi network running VPN is as follows:

- Go through the 7 Steps of Preparation for all deployments
- Select WPA-Enterprise or WPA2-Enterprise Wi-Fi CERTIFIED APs
- Select WPA-Enterprise or WPA2-Enterprise Wi-Fi CERTIFIED client devices
- Follow installation directions according to the manufacturer

Figure 3.3 Upgrading from VPN to WPA




After the entire network is upgraded to WPA or WPA2, VPN can be eliminated for Wi-Fi managed networks. Continuing to use VPN presents a number of disadvantages:

- Users typically experience a noticeable drag on performance when the VPN tunnel is opened
- VPN entails additional hardware and management costs
- VPN offers limited roaming capability
- VPN makes the login process more complex for users and poses throughput issues when used for Voice over IP (VOIP)

**Upgrading from WPA to WPA2**

WPA2 offers a graceful transition path from WPA or a viable solution for new Wi-Fi deployments. In any WPA to WPA2 deployment, managers will have already completed most of the 7 Steps to Prepare for a WPA or WPA2 Deployment and will not have to complete them again. The EAP types now in use can continue to be used with WPA2.

WPA2 allows for an orderly and gradual transition from WPA by offering a highly secure “WPA2 Mixed Mode” that will support the secure co-existence of both WPA and WPA2 client workstations on the network. WPA2 Mixed Mode defaults to WPA TKIP encryption. This allows managers to upgrade clients and access points as part of the enterprise’s normal refresh cycle while maintaining the minimum security of WPA. Managers can make the transition to WPA2 clients and APs gradually, seamlessly, and with a high level of confidence that wireless network security will not be compromised.

Enterprises that require the additional protection of AES-based WPA2 and IEEE 802.11i should begin planning that migration as they deploy WPA. A hardware upgrade may be required to implement the AES portion of WPA2. Many products that are currently available are AES-ready with planned support for WPA2 built into the devices. Other products may not be able to be upgraded to WPA2. Managers should talk to their vendor to see if new firmware or hardware is needed to implement the AES portion of WPA2.

**Summary**

Managers should review the deployment scenarios outlined in this section and follow the one that best describes their migration path to WPA or WPA2. If upgrading to WPA2 from WPA, managers should begin planning the migration strategy now. There is no reason not to deploy WPA or WPA2 today to enjoy the tremendous productivity and benefits of a secure Wi-Fi network.