CISCO SYSTEMS

Cisco **SAFE**: Wireless LAN Security in Depth

Authors

Sean Convery (CCIE #4232), Darrin Miller (CCIE #6447), and Sri Sundaralingam are the primary authors of this white paper. Mark Doering, Pej Roshan, Stacey Albert, Bruce McMurdo, and Jason Halpern provided significant contributions to this paper and are the lead architects of Cisco's reference implementation in San Jose, California, USA. All are network architects who focus on wireless LAN, VPN, or security issues.

Abstract

This paper provides best-practice information to interested parties for designing and implementing wireless LAN (WLAN) security in networks utilizing elements of the Cisco SAFE Blueprint for network security. All SAFE white papers are available at the SAFE Web site:

http://www.cisco.com/go/safe

These documents were written to provide best-practice information on network security and virtual-private-network (VPN) designs. Although you can read this document without having read either of the two primary security design documents, it is recommended that you read either "SAFE Enterprise" or "SAFE Small, Midsize and Remote-User Networks" before continuing.

This paper frames the WLAN implementation within the context of the overall security design. SAFE represents a system-based approach to security and VPN design. This type of approach focuses on overall design goals and translates those goals into specific configurations and topologies. In the context of wireless, Cisco recommends that you also consider network design elements such as mobility

and quality of service (QoS) when deciding on an overall WLAN design. SAFE is based on Cisco products and those of its partners.

This document begins with an overview of the architecture, and then details the specific designs under consideration. Because this document revolves around two principal design variations, these designs are described first in a generic sense, and then are applied to SAFE. The following designs are covered in detail:

- Large-network WLAN design
- Medium-network WLAN design
- Small-network WLAN design
- Remote-user WLAN design

Each design may have multiple modules that address different aspects of WLAN technology. The concept of modules is addressed in the SAFE security white papers.

Following the discussion of the specific designs, Appendix A details the validation lab for SAFE wireless and includes configuration snapshots. Appendix B is a primer on WLAN. If you are unfamiliar with basic WLAN concepts, you should read this section before the rest of the

document. Appendix C provides more details on rogue access point detection and prevention techniques. Finally, Appendix D discusses high availability design criteria for services such as RADIUS and DHCP in order to secure WLANs.

Audience

Though this document is technical in nature, it can be read at different levels of detail, depending on your level of interest. A network manager, for example, can read the introductory sections in each area to obtain a good overview of security design strategies and consideration for WLAN networks. A network engineer or designer can read this document in its entirety and gain design information and threat analysis details, which are supported by actual configuration snapshots for the devices involved. Because this document covers a wide range of WLAN deployments, it may be helpful to read the introductory sections of the paper first and then skip right to the type of WLAN you are interested in deploying.

Caveats

This document presumes that you already have a security policy in place. Cisco Systems does not recommend deploying WLANs—or any networking technology—without an associated security policy. Although network security fundamentals are mentioned in this document, they are not described in detail. Security within this document is always mentioned as it pertains to WLANs.

Even though WLANs introduce security risks, many organizations choose to deploy WLANs because they bring user productivity gains and simplify deployment of small networks. Following the guidelines in this document does not guarantee a secure WLAN environment, nor does it guarantee that you will prevent all penetrations. By following the guidelines, you will mitigate WLAN security risks as much as possible.

Though this document contains a large amount of detail on most aspects of wireless security, the discussion is not exhaustive. In particular, the document does not address wireless bridges, personal digital assistants (PDAs), or non-802.11-based WLAN technology. In addition, it does not provide specific best practices on general WLAN deployment and design issues that are not security related.

During the validation of SAFE, real products were configured in the exact network implementation described in this document. Specific configuration snapshots from the lab are included in Appendix A, "Validation Lab."

Throughout this document the term "hacker" denotes an individual who attempts to gain unauthorized access to network resources with malicious intent. Although the term "cracker" is generally regarded as the more accurate word for this type of individual, hacker is used here for readability.

Architecture Overview

Design Fundamentals

Cisco SAFE wireless emulates as closely as possible the functional requirements of today's networks. Implementation decisions varied, depending on the network functionality required. However, the following design objectives, listed in order of priority, guided the decision-making process:

- Security and attack mitigation based on policy
- Authentication and authorization of users to wired network resources

- Wireless data confidentiality
- User differentiation
- Access point management
- Authentication of users to network resources
- Options for high availability (large enterprise only)

First and foremost, SAFE wireless needs to provide a secure WLAN connectivity option to enterprise networks. As a connectivity option, WLAN access must adhere to an organization's security policy as closely as possible. In addition, it must provide this access as securely as possible while recognizing the need to maintain as many of the characteristics of a traditional wired LAN as possible. Finally, WLANs must integrate with existing network designs based on the SAFE security architecture.

SAFE WLAN Axioms

Wireless Networks Are Targets

Wireless networks have become one of the most interesting targets for hackers today. Organizations today are deploying wireless technology at a rapid rate, often without considering all security aspects. This rapid deployment is due, in part, to the low cost of the devices, ease of deployment, and the large productivity gains. Because WLAN devices ship with all security features disabled, increasing WLAN deployments have attracted the attention of the hacker community. Several Web sites document freely available wireless connections throughout the United States.

Although most hackers are using these connections as a means to get free Internet access or to hide their identity, a smaller group sees this situation as an opportunity to break into networks that otherwise might have been difficult to attack from the Internet. Unlike a wired network, a WLAN sends data over the air and may be accessible outside the physical boundary of an organization. When WLAN data is not encrypted, the packets can be viewed by anyone within radio frequency range. For example, a person with a Linux laptop, a WLAN adapter, and a program such as TCPDUMP can receive, view, and store all packets circulating on a given WLAN.

Interference and Jamming

It is also easy to interfere with wireless communications. A simple jamming transmitter can make communications impossible. For example, consistently hammering an access point with access requests, whether successful or not, will eventually exhaust its available radio frequency spectrum and knock it off the network. Other wireless services in the same frequency range as a WLAN can reduce the range and usable bandwidth of the WLAN. "Bluetooth" technology, used to communicate between handsets and other information appliances, is one of many technologies today that use the same 2.4-GHz radio frequency as WLAN devices and can interfere with WLAN transmissions.

MAC Authentication

WLAN access points can identify every wireless card ever manufactured by its unique Media Access Control (MAC) address that is burned into and printed on the card. Some WLANs require that the cards be registered before the wireless services can be used. The access point then identifies the card by the user, but this scenario is complex because every access point needs to have access to this list. Even if it were implemented, it cannot account for hackers who use WLAN cards that can be loaded with firmware that does not use the built-in MAC address, but a randomly chosen, or deliberately spoofed, address. Using this spoofed address, a hacker can attempt to inject network traffic or spoof legitimate users.

Ad Hoc Versus Infrastructure Modes

Most WLANs deployed by organizations operate in a mode called "infrastructure." In this mode, all wireless clients connect through an access point for all communications. You can, however, deploy WLAN technology in a way that forms an independent peer-to-peer network, which is more commonly called an ad hoc WLAN. In an ad hoc WLAN, laptop or desktop computers that are equipped with compatible WLAN adapters and are within range of one another can share files directly, without the use of an access point. The range varies, depending on the type of WLAN system. Laptop and desktop computers equipped with 802.11b or 802.11a WLAN cards can create ad hoc networks if they are within at least 500 feet of one another.

The security impact of ad hoc WLANs is significant. Many wireless cards, including some shipped as a default item by PC manufacturers, support ad hoc mode. When adapters use ad hoc mode, any hacker with an adapter configured for ad hoc mode and using the same settings as the other adapters may gain unauthorized access to clients.

Denial or Degradation of Service

802.11 management messages including the beacon, probe request or response, association request or response, re-association request or response, disassociation, and de-authentication are not authenticated. Without authenticating these management messages, denial-of-service (DoS) attacks are possible. An example of this type of DoS attack has been demonstrated with open source tools such as wlan-jack.

Wireless Networks Are Weapons

A rogue access point is one that is accessible to an organization's employees but is not managed as a part of the trusted network. Most rogue access points are installed by employees for which IT is not providing WLAN access. A typical rogue access point, then, is an inexpensive one that an employee purchases and installs by plugging it into an available switch port, often with no security measures enabled. A hacker, even one outside the physical boundaries of an organization's facilities, can gain access to the trusted network simply by associating with a rogue access point. Another type of rogue access point is one that masquerades as a trusted access point and tricks WLAN users into associating with it, thereby enabling a hacker to manipulate wireless frames as they cross the access point.

The threat posed by rogue access points can be mitigated by preventing their deployment and detecting those rogue access points that are deployed. The following components are required in order to mitigate the threat of rogue access points. A detailed discussion of these points can be found in Appendix C, "Rogue Access Point Additional Information."

Prevention

- Corporate policy
- Physical security
- Supported WLAN infrastructure
- 802.1X port-based security on edge switches

Detection

- Using wireless analyzers or sniffers
- Using scripted tools on the wired infrastructure
- Physically observing WLAN access point placement and usage

802.11 Is Insecure

As discussed in the primer (Appendix B), 802.11b and 802.11a are the most widely deployed WLAN technologies today. Traditional 802.11 WLAN security includes the use of open or shared-key authentication and static wired equivalent privacy (WEP) keys. This combination offers a rudimentary level of access control and privacy, but each element can be compromised. The following sections describe these elements and the challenges of their use in enterprise environments.

Authentication

The 802.11 standard supports two means of client authentication: open and shared-key authentication. Open authentication involves little more than supplying the correct service set ID (SSID). With open authentication, the use of WEP prevents the client from sending data to and receiving data from the access point, unless the client has the correct WEP key. With shared-key authentication, the access point sends the client device a challenge text packet that the client must then encrypt with the correct WEP key and return to the access point. If the client has the wrong key or no key, authentication will fail and the client will not be allowed to associate with the access point. Shared-key authentication is not considered secure because a hacker who detects both the clear text challenge and the same challenge encrypted with a WEP key can decipher the WEP key.

Key Management

Another type of key that is often used—but is not considered secure—is a "static" WEP key. A static WEP key is a key composed of either 40 or 128 bits that is statically defined by the network administrator on the access point and all clients that communicate with the access point. When static WEP keys are used, a network administrator must perform the time-consuming task of entering the same keys on every device in the WLAN.

If a device that uses static WEP keys is lost or stolen, the possessor of the stolen device can access the WLAN. An administrator will not be able to detect that an unauthorized user has infiltrated the WLAN until and unless the theft is reported. The administrator must then change the WEP key on every device that uses the same static WEP key used by the missing device. In a large enterprise WLAN with hundreds or even thousands of users, this can be a daunting task. Worse still, if a static WEP key is deciphered through a tool such as AirSnort, the administrator has no way of knowing that the key has been compromised by a hacker.

WEP

The 802.11 standards define WEP as a simple mechanism to protect the over-the-air transmission between WLAN access points and network interface cards (NICs). Working at the data link layer, WEP requires that all communicating parties share the same secret key. To avoid conflicting with U.S. export controls that were in effect at the time the standard was developed, 40-bit encryption keys were required by IEEE 802.11b, though many vendors now support the optional 128-bit standard. WEP can be easily cracked in both 40- and 128-bit variants by using off-the-shelf tools readily available on the Internet. On a busy network, 128-bit static WEP keys can be obtained in as little as 15 minutes, according to current estimates. These attacks are described in more detail in the following paragraphs.

As mentioned in the primer (Appendix B), WEP uses the RC4 stream cipher that was invented by Ron Rivest of RSA Data Security, Inc. (RSADSI) for encryption. The RC4 encryption algorithm is a symmetric stream cipher that supports a variable-length key. The IEEE 802.11 standard describes the use of the RC4 algorithm and key in WEP, but does not specify specific methods for key distribution. Without an automated method for key distribution, any encryption protocol will have implementation problems because of the potential for human error in key input, escrow, and management. As discussed later in this document, 802.1X has been ratified in the IEEE and is being embraced by the WLAN vendor community as a potential solution for this key distribution problem.

The initialization vector is at the center of most of the issues that involve WEP. Because the initialization vector is transmitted as plaintext and placed in the 802.11 header, anyone sniffing a WLAN can see it. At 24 bits long, the initialization vector provides a range of 16,777,216 possible values. A University of California, Berkeley paper found that when the same initialization vector is used with the same key on an encrypted packet (known as an initialization-vector collision), a hacker can capture the data frames and derive information about the data as well as the network. For more information, refer to the paper at:

http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html

In the past year, encryption analysts from the University of California, Berkeley, the University of Maryland, and Cisco Systems, Inc. have reported weaknesses in the authentication and WEP encryption schemes in the IEEE 802.11 WLAN standard. These researchers have called for sophisticated key management solutions to mitigate these flaws. The University of Maryland paper can be found at:

http://www.cs.umd.edu/~waa/wireless.pdf

Cryptanalysts Fluhrer, Mantin, and Shamir (FMS) discovered inherent shortcomings with the RC4 key-scheduling algorithm. Because RC4 as implemented in WEP uses a 24-bit initialization vector and does not dynamically rotate encryption keys, these shortcomings are demonstrated to have practical applications in decrypting 802.11 frames using WEP. The attack illustrated in the paper focuses on a large class of weak initialization vectors that can be generated by RC4, and highlights methods to break the key using certain patterns in the initialization vectors. This attack is pragmatic, but the most disconcerting fact is that the attack is completely passive. In this paper, this attack is known as the FMS attack. The FMS attack discusses the theoretical derivation of a WEP key in a range of 100,000 to 1,000,000 packets encrypted using the same key. More detail can be found in the paper itself at:

http://www.cs.umd.edu/~waa/class-pubs/rc4_ksaproc.ps

Recent practical implementations of the FMS attack have been able to derive a static WEP key by capturing about a million packets. This is demonstrated in a paper by AT&T Labs and Rice University at the following URL:

http://www.cs.rice.edu/~astubble/wep/wep_attack.pdf

Several independent developers then released their own implementations of the FMS attack; the most popular of these is AirSnort, which can be downloaded at the following URL:

http://airsnort.sourceforge.net/

Although traditional WLAN security that relies on open or shared keys and static WEP keys is better than no security at all, it is not sufficient for the enterprise organization. Only very small businesses, or those that do not entrust mission-critical data to their WLAN networks, can rely on these WLAN security types. All other enterprises and organizations must invest in a robust, enterprise-class WLAN security solution.

Security Extensions Are Required

Cisco agrees with the findings of the research papers discussed in the previous axiom and recommends deploying elements of the three technologies discussed in this axiom as an alternative to WEP as specified by IEEE 802.11. The technologies discussed include a network layer encryption approach based on IP security (IPsec), a mutual authentication-based, key distribution method using 802.1X, and some proprietary improvements to WEP recently implemented by Cisco. Additionally, IEEE 802.11 Task Group "i" and the Wi-Fi Alliance compliance testing committee are working on standardizing WLAN authentication and encryption improvements.

IPsec

IPsec is a framework of open standards for ensuring secure private communications over IP networks. IPsec VPNs use the services defined within IPsec to ensure confidentiality, integrity, and authenticity of data communications across public networks, such as the Internet. IPsec also has a practical application to secure WLANs by overlaying IPsec on top of cleartext 802.11 wireless traffic.

When deploying IPsec in a WLAN environment, an IPsec client is placed on every PC connected to the wireless network and the user is required to establish an IPsec tunnel to route any traffic to the wired network. Filters are put in place to prevent any wireless traffic from reaching any destination other than the VPN gateway and Dynamic Host Configuration Protocol (DHCP) or Domain Name System (DNS) server. IPsec provides for confidentiality of IP traffic, as well as authentication and anti-replay capabilities. Confidentiality is achieved through encryption using a variant of the Data Encryption Standard (DES), called Triple DES (3DES), or the new Advanced Encryption Standard (AES).

Though IPsec is used primarily for data confidentiality and device authentication, extensions to the standard allow for user authentication and authorization to occur as part of the IPsec process. For more information on IPsec, refer to the VPN primer in the SAFE VPN paper at the following URL:

http://www.cisco.com/go/safe

802.1X/EAP

An alternative WLAN security approach focuses on developing a framework for providing centralized authentication and dynamic key distribution. This approach is based on the IEEE 802.11 Task Group "i" end-to-end framework using 802.1X and the Extensible Authentication Protocol (EAP) to provide this enhanced functionality. Cisco has incorporated 802.1X and EAP into its WLAN security solution—the Cisco Wireless Security Suite. The three main elements of an 802.1X and EAP approach follow:

- Mutual authentication between client and authentication (Remote Access Dial-In User Service [RADIUS]) server
- Encryption keys dynamically derived after authentication
- Centralized policy control, where session time-out triggers reauthentication and new encryption key generation

When these features are implemented, a wireless client that associates with an access point cannot gain access to the network until the user performs a network logon. After association, the client and the network (access point or RADIUS server) exchange EAP messages to perform mutual authentication, with the client verifying the RADIUS server credentials, and vice versa. An EAP supplicant is used on the client machine to obtain the user credentials (user ID and password, user ID and one-time password [OTP], or digital certificate). Upon successful client and server mutual authentication, the RADIUS server and client then derive a client-specific WEP key to be used by the client for the current logon session. User passwords and session keys are never transmitted in the clear, over the wireless link.

The sequence of events follows (refer to Figure 1):

- A wireless client associates with an access point.

- The access point blocks all attempts by the client to gain access to network resources until the client logs on to the network.

- The user on the client supplies network login credentials (user ID and password, user ID and OTP, or user ID and digital certificate) via an EAP supplicant.

- Using 802.1X and EAP, the wireless client and a RADIUS server on the wired LAN perform a mutual authentication through the access point in two phases. In the first phase of EAP authentication, the RADIUS server verifies the client credentials, or vice versa. In the second phase, mutual authentication is completed by the client verifying the RADIUS server credential, or vice versa.

- When mutual authentication is successfully completed, the RADIUS server and the client determine a WEP key that is distinct to the client. The client loads this key and prepares to use it for the logon session.

- The RADIUS server sends the WEP key, called a session key, over the wired LAN to the access point.

- The access point encrypts its broadcast key with the session key and sends the encrypted key to the client, which uses the session key to decrypt it.

- The client and access point activate WEP and use the session and broadcast WEP keys for all communications during the remainder of the session or until a time-out is reached and new WEP keys are generated.

- Both the session key and broadcast key are changed at regular intervals. The RADIUS server at the end of EAP authentication specifies session key time-out to the access point and the broadcast key rotation time can be configured on the access point.

Figure 1
EAP Authentication Process
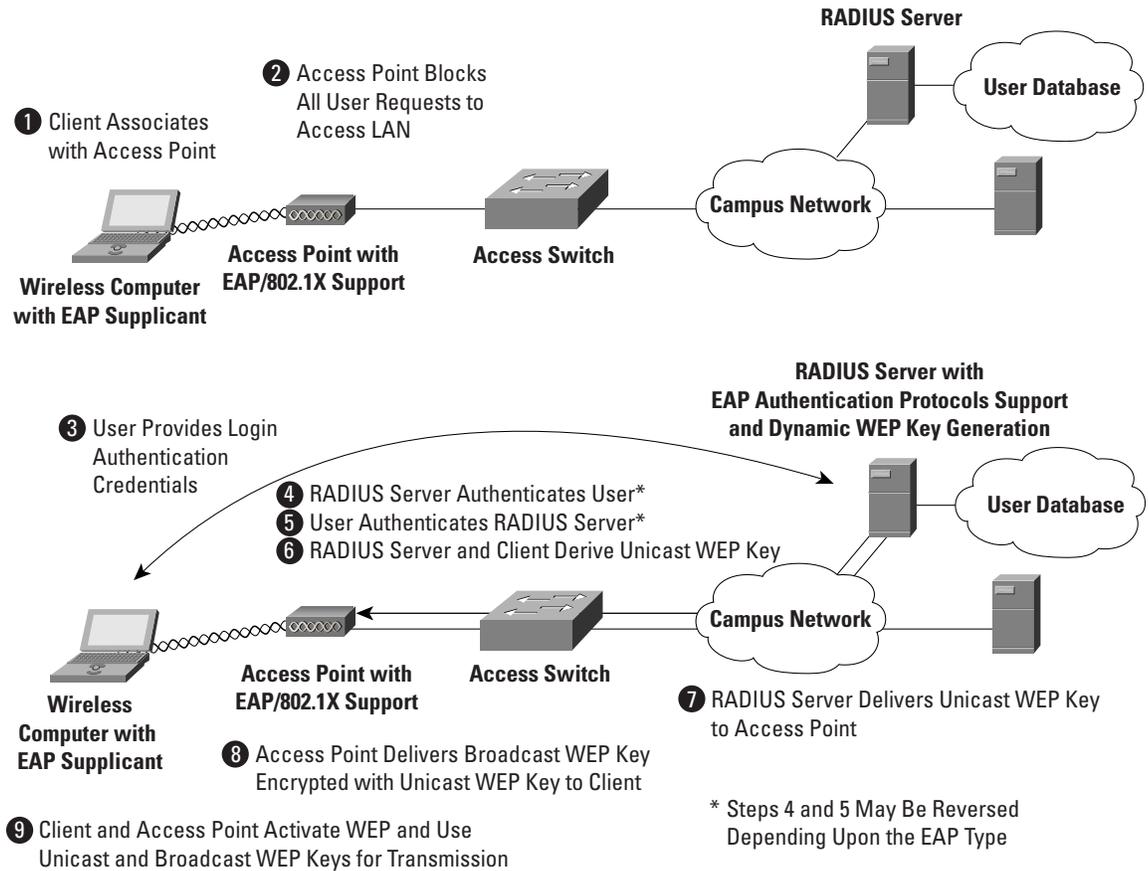
EAP provides three significant benefits over basic 802.11 security:

- The first benefit is the mutual authentication scheme, as described previously. This scheme effectively eliminates "man-in-the-middle (MITM) attacks" introduced by rogue access points and RADIUS servers.

- The second benefit is a centralized management and distribution of encryption keys. Even if the WEP implementation of RC4 had no flaws, there would still be the administrative difficulty of distributing static keys to all the access points and clients in the network. Each time a wireless device was lost, the network would need to be rekeyed to prevent the lost system from gaining unauthorized access.

- The third benefit is the ability to define centralized policy control, where session time-out triggers reauthentication and new key derivation.

EAP Authentication Protocols

Numerous EAP types are available today for user authentication over wired and wireless networks. Current EAP types include:

- EAP-Cisco Wireless (LEAP)
- EAP-Transport Layer Security (EAP-TLS)
- Protected EAP (PEAP)
- EAP-Tunneled TLS (EAP-TTLS)
- EAP-Subscriber Identity Module (EAP-SIM)

In the Cisco SAFE wireless architecture, LEAP, EAP-TLS, and PEAP were tested and documented as viable mutual authentication EAP protocols for WLAN deployments.

Cisco LEAP

Cisco LEAP is the widely deployed EAP type in use today in WLANs. LEAP supports all three of the 802.1X and EAP elements mentioned previously. With LEAP, mutual authentication relies on a shared secret, the user's logon password, which is known by the client and the network. As shown in Figure 2, the RADIUS server sends an authentication challenge to the client. The client uses a one-way hash of the user-supplied password to fashion a response to the challenge and sends that response to the RADIUS server. Using information from its user database, the RADIUS server creates its own response and compares that to the response from the client. When the RADIUS server authenticates the client, the process repeats in reverse, enabling the client to authenticate the RADIUS server. When this is complete, an EAP-Success message is sent to the client and both the client and the RADIUS server derive the dynamic WEP key.

Figure 2
LEAP Authentication Process
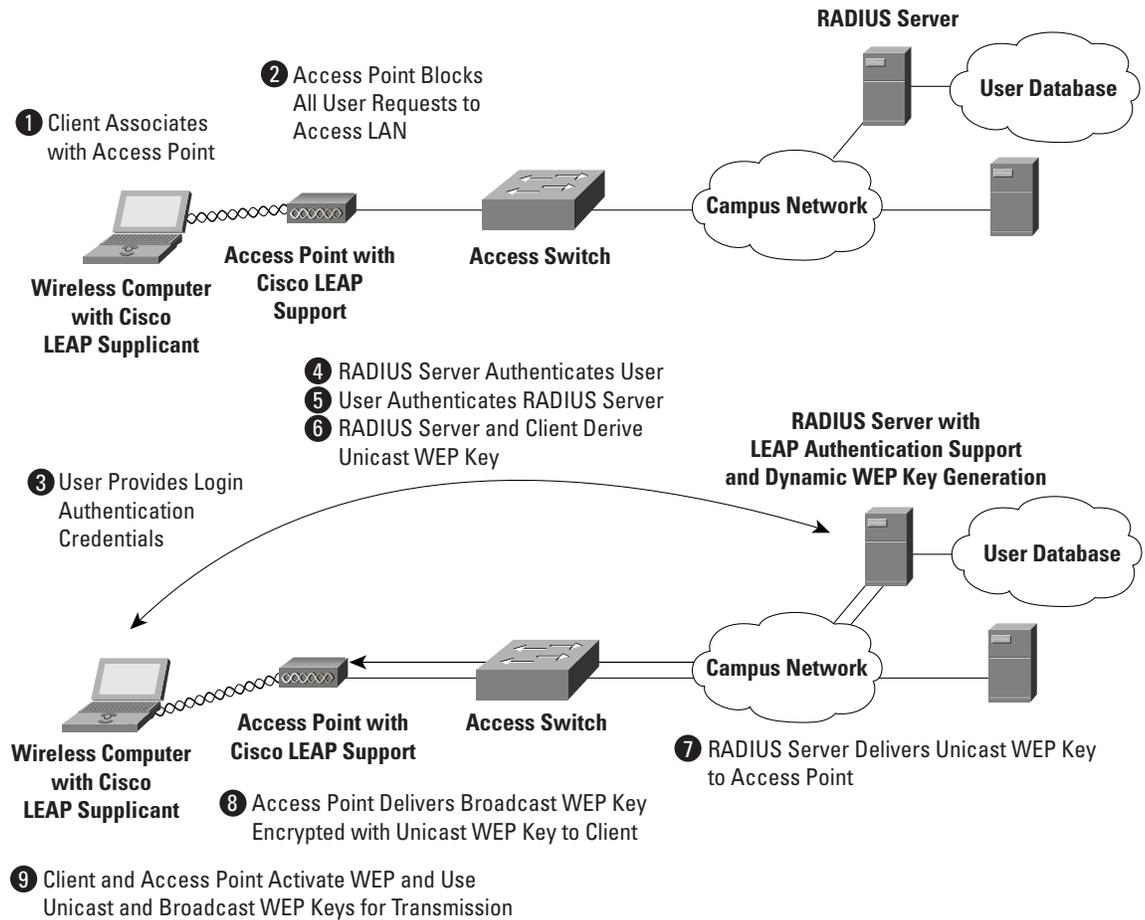
EAP-TLS

EAP-TLS is an Internet Engineering Task Force (IETF) standard (RFC 2716) that is based on the TLS protocol (RFC 2246). EAP-TLS uses digital certificates for both user and server authentication and supports the three key elements of 802.1X/EAP mentioned previously. As shown in Figure 3, the RADIUS server sends its certificate to the client in phase 1 of the authentication sequence (server-side TLS). The client validates the RADIUS server certificate by verifying the issuer of the certificate—a certificate authority server entity—and the contents of the digital certificate. When this is complete, the client sends its certificate to the RADIUS server in phase 2 of the authentication sequence (client-side TLS). The RADIUS server validates the client's certificate by verifying the issuer of the certificate (certificate authority server entity) and the contents of the digital certificate. When this is complete, an EAP-Success message is sent to the client and both the client and the RADIUS server derive the dynamic WEP key.

Figure 3
EAP-TLS Authentication Process
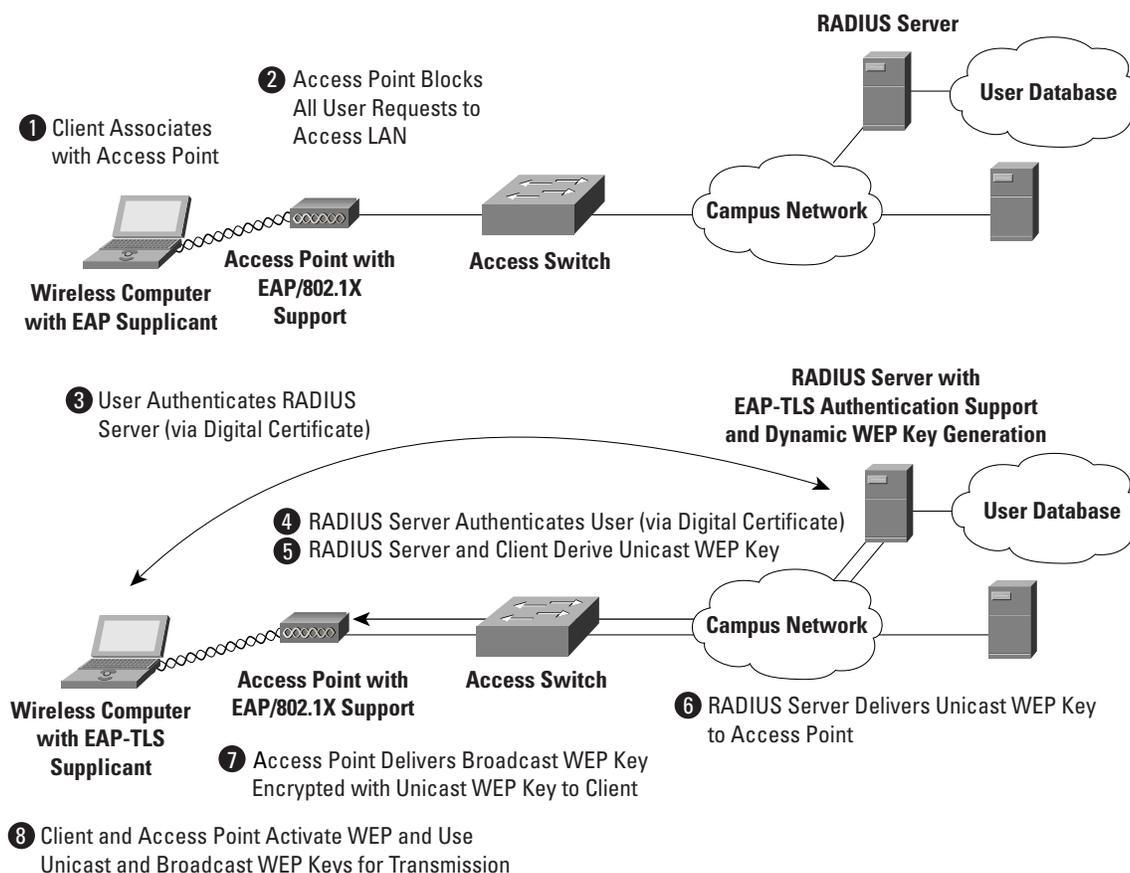
PEAP

PEAP is an IETF draft RFC authored by Cisco Systems, Microsoft, and RSA Security. PEAP uses a digital certificate for server authentication. For user authentication, PEAP supports various EAP-encapsulated methods within a protected TLS tunnel. PEAP supports the three main elements of 802.1X/EAP, as mentioned previously. As shown in Figure 4, phase 1 of the authentication sequence is the same as that for EAP-TLS (server-side TLS). At the end of phase 1, an encrypted TLS tunnel is created between the user and the RADIUS server for transporting EAP authentication messages. In phase 2, the RADIUS server authenticates the client through the encrypted TLS tunnel via another EAP type. As an example, a user can be authenticated using an OTP using the EAP-GTC subtype (as defined by the PEAP DRAFT). In this case, the RADIUS server will relay the OTP credentials (user ID and OTP) to an OTP server to validate the user login. When this is complete, an EAP-Success message is sent to the client and both the client and the RADIUS server derive the dynamic WEP key. For more information on PEAP, refer to the IETF Web site for the latest draft.

Figure 4
PEAP Authentication Process
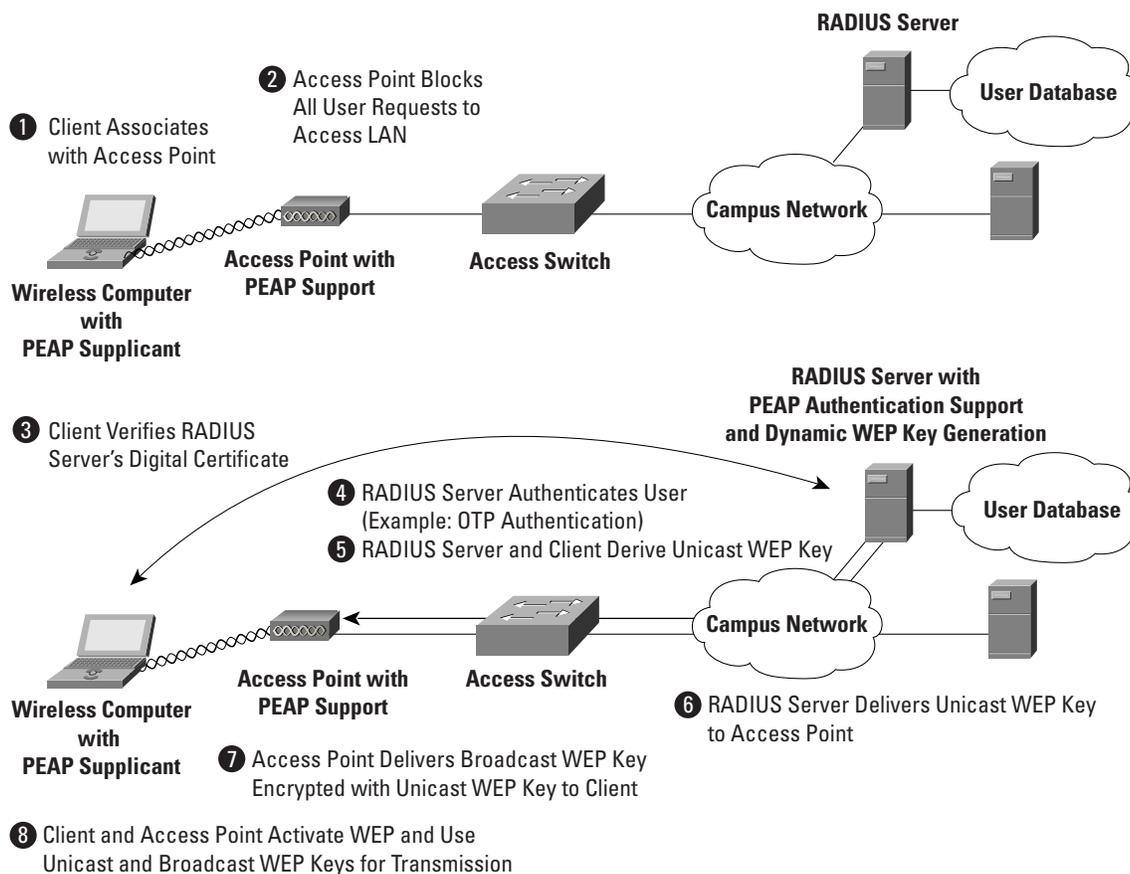
For more information on EAP protocols, implementation details, and guidelines for deployment over WLANs, refer to:

http://www.cisco.com/warp/public/779/smbiz/wireless/wlan_security.shtml/

WEP Enhancements

Enhancements are needed to mitigate the WEP vulnerabilities discussed in the "802.11 Is Insecure" axiom section. IEEE 802.11i includes two encryption enhancements in its draft standard for 802.11 security:

1. Temporal Key Integrity Protocol, or TKIP, which is a set of software enhancements to RC4-based WEP

2. AES, which is a stronger alternative to RC4

In December 2001, Cisco introduced support for TKIP as a component of the Cisco Wireless Security Suite. Because the standard for TKIP was not finalized at that time, the implementation is prestandard and is sometimes referred to as Cisco TKIP. In 2002, 802.11i finalized the specification for TKIP, and the Wi-Fi Alliance announced that it was making TKIP a component of Wi-Fi Protected Access (WPA), which will become a requirement for Wi-Fi compliance before the end of 2003. The enterprise version of WPA also requires 802.1X for 802.11. Both Cisco TKIP and the

WPA TKIP include per-packet keying (PPK) and message integrity check (MIC). WPA TKIP introduces a third element: extension of the initialization vector from 24 bits to 48 bits. This section discusses the Cisco TKIP implementation details that demonstrate the security enhancements of TKIP. For more information on WPA, refer to the WECA Web site:

http://www.weca.net

Cisco TKIP: Per-Packet Keying

Because the most popular attack against WEP relies on exploiting multiple weak initialization vectors in a stream of encrypted traffic using the same key, using different keys per packet is a potential way to mitigate the threat. As illustrated in Figure 5, the initialization vector and WEP key are hashed to produce a unique packet key (called a temporal key), which is then combined with the initialization vector and run through a mathematical function called XOR with the plaintext. The standard 802.11 method of doing the RC4 cryptography in WEP is described in the primer (Appendix B).

Figure 5

Per-Packet WEP Key Hashing
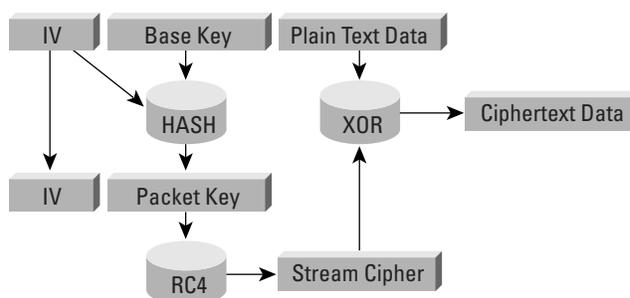
This scenario prevents the weak initialization vectors from being used to derive the base WEP key because the weak initialization vectors allow you to derive only the per-packet WEP key. In order to prevent attacks due to initialization-vector collisions, the base key should be changed before the initialization vectors repeat. Because initialization vectors on a busy network can repeat in a matter of hours, mechanisms like EAP authentication protocols should be used to perform the rekey operation.

Similar to a unicast key, the WLAN broadcast key (used by access points and clients for Layer 2 broadcast and multicast communication) is susceptible to attacks due to initialization vector collisions. Cisco's access points support broadcast key rotation to mitigate this vulnerability. The access point dynamically calculates the broadcast WEP key (as a function of a random number) and the new broadcast WEP key is delivered to clients using EAPOL-Key messages. Thus, broadcast WEP key rotation can be enabled only with EAP protocols such as LEAP, EAP-TLS, and PEAP that support dynamic derivation of encryption keys.

Cisco TKIP—Message Integrity Check

Another concern with WEP is its vulnerability to replay attacks. The MIC protects WEP frames from tampering. The MIC is based on a seed value, destination MAC, source MAC, and payload (that is, any changes to these will affect the MIC value). And the MIC is included in the WEP-encrypted payload. MIC uses a hashing algorithm to derive the resulting value. This is an improvement of the cyclic redundancy check (CRC)-32 checksum function as performed by standards-based WEP. With CRC-32, it is "possible to compute the bit difference of two CRCs based on the bit

difference of the messages over which they are taken. In other words, flipping bit *n* in the message results in a deterministic set of bits in the CRC that must be flipped to produce a correct checksum on the modified message. Because flipping bits carries through after an RC4 decryption, this allows the attacker to flip arbitrary bits in an encrypted message and correctly adjust the checksum so that the resulting message appears valid."

Summary

Organizations should choose to deploy either IPsec or 802.1X/EAP with TKIP or Cisco TKIP, but generally not both. Specific designs using both at the same time were tested in the SAFE lab and are discussed in the "Alternatives" sections of the following designs. Organizations should use IPsec when they have the utmost concern for the sensitivity of the transported data, but remember that this solution is more complex to deploy and manage than 802.1X/EAP with TKIP. The 802.1X/EAP with TKIP should be used when an organization wants reasonable assurance of confidentiality and a transparent user security experience. The basic WEP enhancements can be used anywhere WEP is implemented. For the vast majority of networks, the security provided by 802.1X/EAP with TKIP is sufficient. Table 1 gives a detailed view of the pros and cons of IPsec and EAP authentication protocols in WLAN designs:

Table 1 Wireless Encryption Technology Comparison

	Cisco LEAP with TKIP	EAP-TLS with TKIP	EAP-PEAP with TKIP	IPsec-based VPN
Key length (in bits)	128	128	128	168/128, 192, 256
Encryption algorithm	RC4	RC4	RC4	3DES or AES
Packet integrity	CRC-32/MIC	CRC-32/MIC	CRC-32/MIC	MD5-HMAC/ SHA-HMAC
Device authentication	No	Certificate	No	Pre-shared secret or certificates
User authentication	Username/ password	Certificate	Username/ password or OTP	Username/ Password or OTP
Certificate requirements	None	RADIUS server/ WLAN client	RADIUS server	Optional
User differentiation[1]	Group	Group	Group	User
Single sign-on support	Yes	Yes	No	No
ACL requirements	Optional	Optional	Optional	Required
Additional hardware	No	Certificate server	Certificate server	IPsec Concentrator
Per-user keying	Yes	Yes	Yes	Yes
Protocol support	Any	Any	Any	IP unicast
Client OS support	Wide range	Wide range	Wide range	Wide range
Open standard	No	Yes	IETF draft RFC	Yes

1. User differentiation is discussed further in the section "WLAN User Differentiation."

Network Availability Impacts Wireless

Network designers concerned about designing and implementing highly available wireless networks need to consider both the wired and wireless elements in their design. In Cisco SAFE wireless, this paper discusses only the availability requirements of the network elements that provide security-related services. Specifically, high availability is required for the following three services:

- DHCP
- RADIUS
- IPsec

A more detailed discussion can be found in Appendix D, "Network Availability."

WLAN User Differentiation

In wired networks, it is often possible to segment users by community through the use of Layer 3 segmentation. In SAFE enterprise design, for example, there is a separation between a marketing segment and an R&D segment. This segmentation occurs at the building distribution module, which is the first point of Layer 3 in the network for the user community. Throughout the rest of the SAFE enterprise design, this segmentation can be maintained by filtering on the IP address that the different user communities access. Furthermore, this sort of segmentation can be administratively complex because the functional and physical separations are often two different things. For example, a financial controller with the need to access an organization's accounting systems could be sitting next to a guest cubicle that needs access only to basic services.

Similar to the wired world, user differentiation in the wireless world can be implemented using wireless virtual LANs (VLANs) mapped to wired VLANs. Mixed deployment of security standards (802.1X/EAP and IPsec VPN) are supported through multiple VLANs, each VLAN supporting a specific security scheme. A unique wireless VLAN is identified using a unique SSID and is mapped to a wired VLAN ID. Continuing the example, the financial controller and guest use different SSIDs to obtain network access. Each SSID is mapped to a unique VLAN ID. Furthermore, VLAN access control mechanisms can be implemented using the RADIUS server. For example, the access point can dynamically map the financial controller to a VLAN ID returned by the RADIUS server upon successful 802.1X/EAP authentication. Also, the introduction of VLANs on the access point allows organizations to separate their access point management traffic from the normal flow of user traffic. Refer to Appendix A for an example implementation of user differentiation (Engineering and R&D user groups) in the enterprise EAP design. For more information on VLAN implementation on Cisco wireless platforms, refer to the "Wireless VLAN Deployment Guide" posted on Cisco.com:

http://www.cisco.com/en/US/products/hw/wireless/ps430/prod_technical_reference09186a00801444a1.html

Without the implementation of wireless VLANs, IPsec-based VPN implementation can be used to enforce user-group privileges. By requiring users to run a VPN client on their end hosts, you can use the wireless network purely for transit and allow the VPN to handle any security controls. This design is discussed in detail later in the document.

Design Approach

Cisco SAFE wireless addresses the general concerns of WLAN security as outlined in the axiom section. This design section integrates the concerns and mitigation techniques of the axiom section and applies them to a variety of different networks. The size and security concerns of the specific design dictate the mitigation techniques that are applied to a WLAN design. Therefore, the network designer is offered a choice of the mitigation technology to implement along with the advantages and disadvantages of the technologies specific to the SAFE design. The mitigation technologies are consistent across all the SAFE designs, so a review of the networking elements of each of the two main technology choices is presented first. After reviewing the technologies, the network designer is presented with each SAFE design, along with the advantages and disadvantages of implementing the specific mitigation technologies within SAFE. Any unique characteristics of implementing a mitigation technology within the SAFE designs are also presented. The two main design choices follow:

- Implementing a dynamic WEP keying model using 802.1X/EAP and TKIP
- Implementing an overlay VPN network using IPsec

Standard WLAN Design Guidelines

This section outlines the generic elements of WLAN designs because so many of them are common throughout the SAFE designs. After reading this section, you can move to the WLAN design that most interests you. In this way, the basic concepts can be included once, with specific variances and alternatives discussed in the specific SAFE design. In the standard WLAN designs, it is assumed that all WLAN devices are connected to a unique IP subnet to enable end-user mobility throughout various designs. An assumption is made in the designs that most services available to the wired network are also available to the wireless network addition. All designs include the following WLAN security principles:

- Access point security recommendations:
    - Enable centralized user authentication (RADIUS, TACACS+) for the management interface.
    - Choose strong community strings for Simple Network Management Protocol (SNMP) and change them often.
    - Consider using SNMP Read Only if your management infrastructure allows it.
    - Disable any insecure and nonessential management protocol provided by the manufacturer.
    - Utilize secure management protocols, such as Secure Shell Protocol (SSH).
    - Limit management traffic to a dedicated wired subnet.
    - Isolate management traffic from user traffic and encrypt all management traffic where possible.
    - Enable wireless frame encryption where available.
    - Physically secure the access point.
- Client security recommendations:
    - Disable ad hoc mode.
    - Enable wireless frame encryption where available.

Standard EAP with TKIP WLAN Design

This design details a generic method for using EAP with TKIP as a security mechanism to access the production corporate network (refer to Figure 6).

Figure 6
Attack Mitigation Roles for Standard EAP WLAN Design
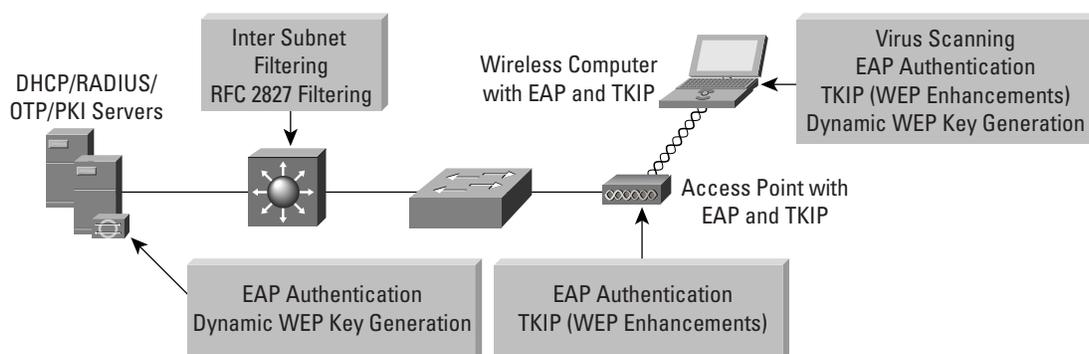
Key EAP Devices

- *Wireless client adapter and software*—A software solution that provides the hardware and software necessary for wireless communications to the access point; it provides mutual authentication to the access point via an EAP mutual authentication type; an EAP supplicant is required on the client machine to support the appropriate EAP authentication type

- *Wireless access point*—Mutually authenticates wireless clients via EAP and can support multiple Layer 2 VLANs for user differentiation

- *Layer 2 or 3 switch*—Provides Ethernet connectivity and Layer 3 or 4 filtering between the WLAN access point and the corporate network

- *RADIUS server*—Delivers user-based authentication for wireless clients and access point authentication to the wireless clients; additionally, the RADIUS server can be used to specify VLAN access control parameters for users and user groups

- *DHCP server*—Delivers IP configuration information for wireless LEAP clients

- *OTP server (optional)*—Authorizes OTP information relayed from the RADIUS server (for PEAP clients only)

- *PKI server (optional)*—Provides X.509v3 digital certificate for user and server identification

Threats Mitigated

- *Wireless packet sniffers*—Wireless packet sniffers can take advantage of any of the known WEP attacks to derive the encryption key. These threats are mitigated by WEP enhancements (specifically per-packet keying as part of TKIP) (see the section "Security Extensions Are Required"), and key rotation using EAP.

- *Unauthenticated access*—Only authenticated users are able to access the wireless and wired network. Optional access control on the Layer 3 switch limits wired network access.

- *MITM*—The mutual authentication nature of several EAP authentication types combined with the MIC can prevent hackers from inserting themselves in the path of wireless communications.

- *IP spoofing*—Hackers cannot perform IP spoofing without first authenticating to the WLAN, after authenticating optional RFC 2827 filtering on the Layer 3 switch restricts any spoofing to the local subnet range.
- *Address Resolution Protocol (ARP) spoofing*—Hackers cannot perform ARP spoofing without first authenticating to the WLAN; after authenticating, ARP spoofing attacks can be launched in the same manner as in a wired environment to intercept other users' data.
- *Network topology discovery*—Hackers cannot perform network discovery if they are unable to authenticate. The attacker can note that a WLAN network exists by looking for or observing the access point SSID, but cannot access the network. When authenticated via EAP, standard topology discovery can occur in the same way that is possible in the wired network.

Threats Not Mitigated

- *Password attack*—Several EAP types take into consideration that an attacker can passively monitor the 802.1X/ EAP exchanges between the client and the access point, and they mitigate this risk via various methods. PEAP mitigates this by establishing a TLS tunnel from the client to the server before asking for user authentication credentials. Also, because EAP-PEAP takes advantage of other EAP types for client-to-server authentication, the designer may choose to implement a strong authentication method such as OTP. EAP-TLS mitigates this via public key cryptography (refer to Table 2).

Table 2 WLAN Security Threat Mitigation by EAP/802.1X with TKIP Deployments

Attack	Cisco LEAP with TKIP	EAP-TLS with TKIP	EAP-PEAP (Client Authentication using OTP) with TKIP
MITM (active attacks)	Mitigated	Mitigated	Mitigated
Authentication forging	Mitigated	Mitigated	Mitigated
Passive attacks (FMS paper)	Mitigated	Mitigated	Mitigated
Rogue access points	Mitigated	Mitigated	Mitigated
Brute-force dictionary attacks	Vulnerable[1]	Mitigated	Mitigated

1. Use of a strong password policy is recommended to mitigate brute-force dictionary attacks against LEAP. The IT administrator also needs to limit the number of login attempts before locking out the account.

EAP with TKIP Design Guidelines

In most cases, WLAN access points are connected to existing Layer 2 access switches. RADIUS and DHCP servers are located in the network services module of the corporate network. Security in the design is maintained by preventing network access to unauthenticated clients, including events of a RADIUS service failure. Because most of the mitigation against security risks relies on the RADIUS service, this behavior is required. Overall, management of the solution is hindered if DHCP services fail. The wireless clients and access points use EAP to authenticate the WLAN client devices and end users against the RADIUS servers. For scalability and manageability purposes, the WLAN client devices are configured to use the DHCP protocol for IP configuration. DHCP occurs after the device and end user are successfully authenticated via an EAP protocol. After successful DHCP configuration, the wireless

end user is allowed access to the corporate network and filtering, if configured, occurs. Network designers should give special consideration to the location of the RADIUS and DHCP servers used by EAP in order to guarantee high availability of the network services for WLAN users.

In order to prevent attacks due to initialization vector collisions, rekeying for both unicast and broadcast keys are recommended. For EAP with Cisco TKIP, rekeying time of 4 hours and 40 minutes is recommended for both unicast and broadcast WEP keys. For more information, refer to white papers posted at:

http://www.cisco.com/warp/public/779/smbiz/wireless/wlan_security.shtml/

Additionally, the network designer should consider RADIUS server scalability in a large design. For example, server load balancing products can be used to load balance between multiple RADIUS servers in a large design.

EAP-protocol specific design guidelines follow:

- For EAP-TLS, it is recommended to use a private PKI to issue digital certificates. This allows for integration of the PKI infrastructure with existing back-end user databases (for example, Microsoft Windows 2000 AD) for certificate management.
- For EAP-TLS and EAP-PEAP, it is recommended to configure wireless clients with the trusted certificate server's digital certificate and to prevent the normal user from modifying these settings. Only the IT administrator should have the privilege levels to modify these settings on the EAP supplicant in a wireless client. If the trusted certificate authority's certificate was not configured, MITM attacks are possible via the use of identity spoofing.
- For EAP-LEAP and EAP-PEAP (when using static passwords), it is recommended that after a small number of incorrect login attempts, the account be locked to prevent brute-force attacks from occurring on the user account. The number of attempts is specified on the RADIUS server, and it is also recommended that these passwords be aged aggressively. The network designer can additionally mitigate this risk by requiring OTPs for client authentication.
- For EAP-TLS, it is recommended to configure the RADIUS server to check the certificate authority's certificate revocation list (CRL) for expired client certificates.

Optionally, network designers could consider implementation of unique wireless VLANs with the EAP design. Dynamic VLAN assignment can be implemented for EAP users using the RADIUS server and user-group settings. This has the advantage of segregating wireless users into user communities and enforcing policies for these groups at the distribution layer. With the use of VLANs on access points, the management traffic can also be isolated from user traffic with the implementation of management VLAN on the access points.

Standard VPN WLAN Design

This design details a generic method for using IPsec VPNs as an overlay security mechanism to access the production corporate network from a WLAN (refer to Figure 7).

Figure 7

Attack Mitigation Roles for Standard VPN WLAN Design
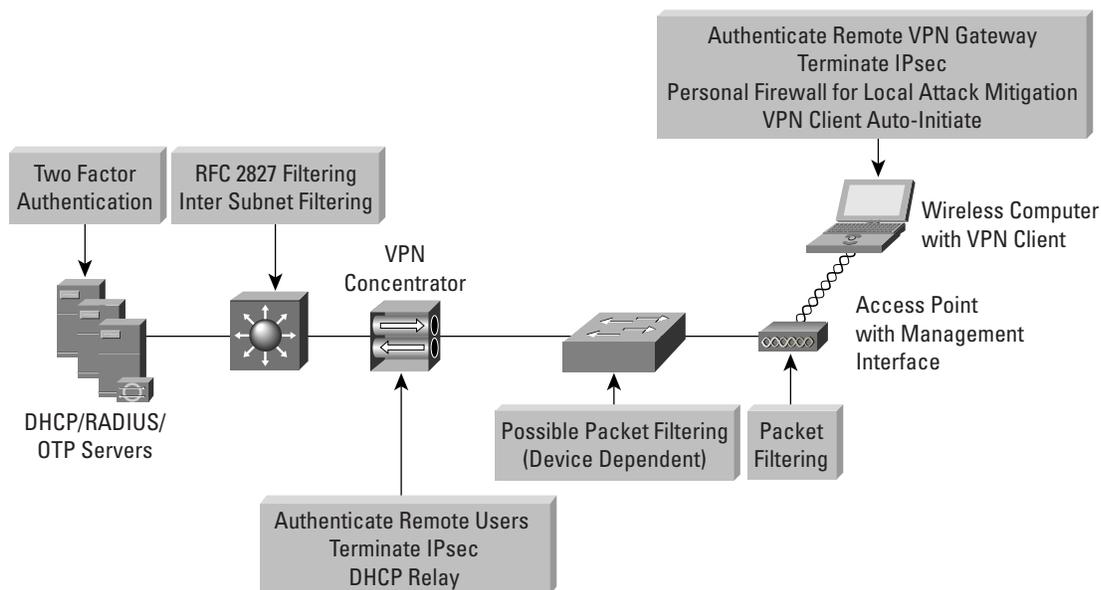
Key VPN Devices

- *Wireless client adapter and software*—A software solution that provides the hardware and software necessary for wireless communications to the access point

- *Remote-access VPN client with personal firewall software*—A software client that provides end-to-end encrypted tunnels between individual PCs and the corporate wireless VPN gateways; personal firewall software provides device-level protection for individual PCs

- *Wireless access point*—Provides initial IP protocol filtering between the WLAN and corporate network

- *Layer 2 switch*—Provides Ethernet connectivity between the WLAN access points and the corporate network; additionally, recent models of access layer switches have the capability to implement a technology called VLAN ACL (VACL), which can provide an additional layer of IPsec filtering

- *Layer 3 switch*—Routes and switches production network data from one module to another; provides additional policy enforcement via protocol-level filtering for wireless traffic

- *RADIUS server*—Authenticates wireless users terminating on the VPN gateway; optionally talks to an OTP server

- *OTP server*—Authorizes OTP information relayed from the RADIUS server

- *DHCP server*—Delivers IP configuration information for wireless VPN clients before and after VPN establishment

- *VPN gateway*—Authenticates individual remote users and terminates their IPsec tunnels and can also provide DHCP relay functionality for wireless clients

Threats Mitigated

- *Wireless packet sniffers*—These threats are mitigated by IPsec encryption of wireless client traffic. Also, new features in VPN client software allow the designer to specify that the VPN tunnel is automatically initiated when the correct WLAN IP address is assigned to the client. This eliminates user interaction to bring up the IPsec tunnel and also protects the client PC from broadcasting traffic onto the wireless media that could be used for inference-based attacks.

- *MITM*—These threats are mitigated by IPsec encryption and authentication of wireless client traffic.

- Unauthorized access—The only known protocols for initial IP configuration (DHCP) and VPN access (DNS, Internet Key Exchange [IKE], and Encapsulating Security Payload [ESP]) are allowed from the WLAN to the corporate network through filtering at the access point and access layer switch. Authorization policies can be optionally enforced on the VPN gateway for individual user groups.

- *IP spoofing*—Hackers can spoof traffic on the WLAN, but only valid, authenticated IPsec packets will ever reach the production wired network.

- *ARP spoofing*—ARP spoofing attacks can be launched; however, data is encrypted to the VPN gateway so hackers will be unable to read the data.

- *Password attacks*—These threats are mitigated through good password policies and auditing and optionally, OTP.

- *Network topology discovery*—Only IKE, ESP, DNS, and DHCP are allowed from this segment into the corporate network. Internet Control Message Protocol (ICMP) is recommended to be allowed only to the outside interface of the VPN concentrator for troubleshooting purposes.

Threats Not Mitigated

- *MAC or IP spoofing from unauthenticated users*—ARP spoofing and IP spoofing are still effective on the WLAN subnet until the wireless client uses IPsec to secure the connection.

Standard VPN WLAN Design Guidelines

WLAN access points connect to Layer 2 switches in the building module on a dedicated wired VLAN and forward IPsec traffic from the WLAN client. The traffic is kept separate from normal wired traffic until it is decrypted by the VPN termination device. It is important to point out that WEP is not enabled in this design. The wireless network itself is considered an untrusted network, suitable only as a transit network for IPsec traffic. In order to isolate this untrusted network, administrators should not mix the VLAN for the WLAN users with a wired network. This configuration would allow hackers on the wireless network to potentially attack users on the wired network. The WLAN clients associate with a wireless access point to establish connectivity to the campus network at Layer 2. The wireless clients then use DHCP and DNS services in the server module to establish connectivity to the campus at Layer 3. After the initial Layer 3 configuration, the VPN tunnel authenticates to the VPN gateway. The VPN gateway can use digital certificates or preshared keys for wireless device authentication. If the VPN gateway uses preshared keys for authentication, then OTPs are recommended to authenticate users to it. Without OTP, the VPN gateways are open to brute-force login attempts by hackers who have obtained the shared IPsec key used by the VPN gateway. The VPN gateway takes advantage of RADIUS services, which in turn contact the OTP server for user authentication. The VPN gateway uses DHCP for IP address configuration in order for the WLAN client to communicate through the VPN tunnel. Security in the design is maintained by preventing network access if a VPN gateway or RADIUS service fails. Both services are required in order for the client to reach the wired network with production traffic. It

should be noted that when the wireless client is communicating with the campus network, but before the IPsec tunnel is established, the client traffic is not considered secure. All the noted WLAN security issues are still present until the wireless client can secure communications with an IPsec VPN. Therefore, three mitigation techniques are recommended:

First, the access point should be configured with EtherType, protocol, and port filters based on a company's wireless usage policy. SAFE WLAN recommends restrictive filters that allow only the necessary protocols required for establishing a secure tunnel to a VPN gateway. These protocols include DHCP for initial client configuration; DNS for name resolution of the VPN gateways; the VPN-specific protocols, IKE (User Datagram Protocol [UDP] port 500) and ESP (IP Protocol 50), and ICMP for troubleshooting purposes. Even with this filtering, the DNS and DHCP servers are still open to direct attack on the application protocols themselves. Extra care should be taken to ensure that these systems are as secure as possible at the host level. This includes keeping them up-to-date with the latest OS and application patches and running a host-based intrusion detection system (HIDS). Additionally, recent models of access layer switches have the capability to implement a technology called VLAN ACL (VACL). Implementing VACLs for VPN-related protocols and specific IP addresses of the VPN concentrators can provide an additional layer of filtering to guarantee that only IPsec traffic destined for the appropriate enterprise VPN concentrators crosses the switch. The DNS traffic is optional, dependent on whether the VPN client needs to be configured with a DNS name for the VPN gateway or if only an IP address is suitable. It is recommended that ICMP be allowed only to the outside interface of the VPN concentrator for troubleshooting purposes and path maximum-transmission-unit (MTU) discovery.

Secondly, a VPN client feature automatically establishes a tunnel when the correct WLAN IP address is received from DHCP. This feature eliminates the need for the end user to manually establish the VPN tunnel after the computer startup. Third, personal firewall software is included on the wireless client to protect the client while it is connected to the untrusted WLAN network without the protection of IPsec. In general terms, the VPN gateway delineates between the trusted wired network and the untrusted WLAN. The wireless client establishes a VPN connection to the VPN gateway to start secure communication to the corporate network. In the process of doing so, the VPN gateway provides device and user authentication via the IPsec VPN. Split tunneling by the client should be disabled—all traffic must traverse the tunnel.

Alternatives

Network designers may still consider enabling static WEP keys on all devices in an effort to add an additional deterrent against hackers. The management overhead of dealing with static key changes makes this alternative less than ideal for large WLAN deployments. This management overhead could be mitigated by never changing the static WEP key, but this solution falls strongly into the "security-through-obscurity" category.

Additionally, network designers can consider using a layering of 802.1X/EAP with the IPsec-based VPN deployment to secure their WLAN environment. The primary drawback with this alternative is the necessity of managing two separate security infrastructures for WLAN deployments.

To further secure the DNS and DHCP services, network designers should consider using dedicated hosts for the VPN WLAN DHCP and DNS deployment. This mitigates against two potential threats that could affect wired resources:

- DoS attacks against the DHCP and DNS services that could affect wired users
- Network reconnaissance through the use of DNS queries or reverse lookups

As an alternative to dedicated DNS servers, designers may consider hard-coding the IP address of the VPN gateway for the VPN clients. The drawback of this solution is if the IP address of the VPN gateway changes, every client will need to update his gateway entry.

Alternative WLAN Security Designs

Alternatively, network designers can also evaluate the feasibility of implementing an application layer security protocol such as Secure Socket Layer (SSL) or a tunneling protocol such as SSH in order to protect their wireless networks. To be implemented effectively in a wireless environment, the protocols need to be deployed using strong mutual authentication in order to mitigate the threat of a MITM attack. This will require the use of client-side certificates when deploying SSL to protect the application layer. Also, it should be noted that SSL is prevalent in most of the enterprise client OSs through a free browser implementation. On the other hand, SSH is not natively supported in most enterprise desktop operating systems. The network designer may have to incur a per-client cost for an SSH client. Cisco does not recommend SSL or SSH in SAFE wireless because of the limited number of technologies that can easily be secured with these protocols.

Large-Enterprise WLAN Design

The large-enterprise WLAN design overlays WLANs on top of the campus portion of the SAFE enterprise blueprint. All the components for implementing the mitigation techniques are contained within the large-enterprise building, distribution, and server modules. These components are intended to allow WLAN access for enterprise end users within the enterprise campus. Specifics for implementing each mitigation technique are discussed in detail in the following sections.

Design Guidelines

In the large-enterprise WLAN design, scalability and high availability were primary concerns when implementing the mitigation technologies. Both LEAP and VPN are considered viable security options for large-enterprise WLAN designs. Network designers should weigh the business benefits of both technologies with the company security policy before selecting the technology that is best suited for their network.

Network Management

In order to isolate management traffic from user traffic, it is recommended to use VLANs on the access points, creating a management VLAN for the access points and restricting access to the access points via the management subnet by implementing ACLs in the building distribution Layer 3 switch. The ACLs should be specific to the IP address and protocols that the centralized multidevice access point configuration tool requires. Note that because access points support only one wired interface, all management was done in band, versus the out-of-band management as recommended by SAFE enterprise. This setup contains a security risk because some management traffic (SNMP, Trivial File Transfer Protocol [TFTP], Hypertext Transfer Protocol [HTTP]) must be sent in the clear in order to manage each access point via a central management station. The access point should be configured to provide central authentication, authorization, and accounting (AAA) of access point administrators via RADIUS or TACACS+, depending on the support of the deployed access points. Finally, network administrators should utilize a secure management transport such as SSH in order to manage the access points from the command line.

EAP with TKIP Option

Figure 8

Large-Enterprise EAP WLAN Design
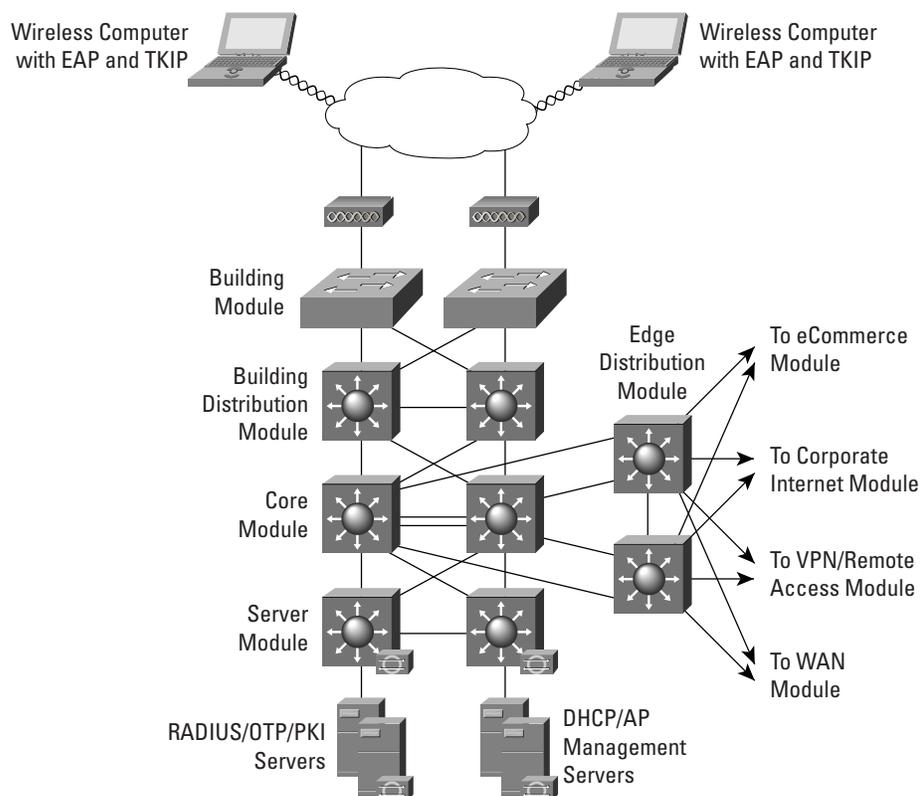
EAP access via the wireless network takes advantage of three components from the SAFE enterprise architecture:

- Building module
- Building distribution module
- Server module

In the large WLAN design, the wireless access points are connected to existing Layer 2 access switches in the building module throughout the corporate campus. RADIUS OTP, PKI, and DHCP servers are located in the server module. The primary concern for EAP in a large WLAN design is the availability and scalability of the network configuration and authentication servers. Following the notes in the axiom section, the RADIUS, OTP, PKI, and DHCP servers are deployed in a redundant fashion on differing network subnets to ensure high availability and scalability. Additionally, server load balancing products can increase the scalability of the RADIUS servers by spreading the RADIUS authentication requests evenly across a farm of RADIUS servers. Beyond the notes listed previously, the connectivity method is identical to the standard EAP WLAN design discussed earlier in the document.

Alternatives

As discussed in the general EAP design guidelines section, EAP design along with VLANs on the access points enables the network designer to implement user differentiation (using wired and wireless VLANs) and enforce VLAN assignment for users and user groups using the RADIUS server. Additionally, the network designer has the option to create a guest VLAN in order to allow guests of the enterprise access to the corporate network to gain access to a limited set of resources or VPN across the Internet to gain access to the guest's corporate network. In either of these cases, it is recommended that the network designer implement packet filters on the access and Layer 3 building distribution switch (or wherever the guest VLAN is terminated) to allow only traffic that conforms to the enterprise guest security policy (that is, IPsec traffic only). Similarly, a VLAN can be created for traditional wireless devices that support only static WEP, and an appropriate security policy can be enforced for this VLAN as well. Refer to Appendix A for an example of implementation of EAP design with the use of VLANs on the access points.

IPsec VPN Option

Figure 9

Large-Enterprise VPN WLAN Design
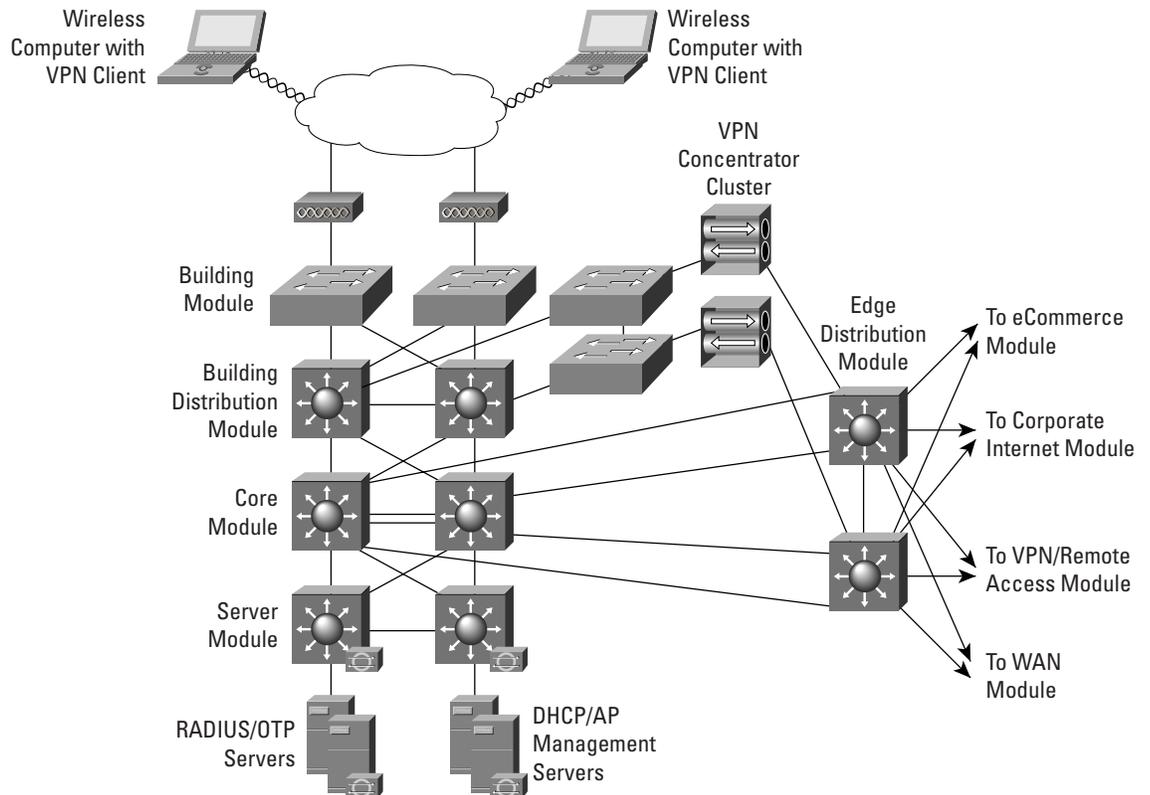
IPsec VPN access via the wireless network uses several modules from the SAFE enterprise architecture:

- Building module
- Building distribution module
- Edge distribution module
- Server module

Design Guidelines

The primary objective in the large WLAN design involves balancing mitigating security risks with creating a scalable design that a business can afford to implement. The standard VPN WLAN design guidelines in this document outlined the general way the VPN can be implemented to secure a WLAN environment. In the context of a large WLAN environment, the guidelines described would be cost-prohibitive for most businesses because of the requirement for a separate Layer 2 switching infrastructure and cabling. Therefore, security trade-offs are made in order to make a VPN WLAN feasible in a large environment. These trade-offs are noted in the following paragraphs to help network designers decide if VPNs are a proper solution for their environment.

The WLAN clients associate with a wireless access point in the building module to establish connectivity to the campus network at Layer 2. The wireless clients then use DHCP and DNS services in the server module to establish connectivity to the campus at Layer 3. It should be noted that when the wireless client is communicating with the WLAN network, but before the IPsec tunnel is established, the client traffic is not considered secure. All the noted WLAN security issues are still present until the wireless client can secure communications with an IPsec VPN. The auto-initiate feature of the VPN client should be utilized in order to minimize the amount of time before the VPN tunnel is established. In addition to the filters on the access point noted in the general VPN WLAN design, the building distribution module Layer 3 switches are configured with ACLs to permit only protocols necessary for VPN connectivity and management. The wireless client establishes a VPN connection to the VPN gateways connecting the building distribution and edge distribution modules. The redundant VPN gateways are configured in a load-balancing configuration to provide high availability and scalability. These VPN gateways are a centralized resource shared by potentially multiple Layer 2 building modules. The RADIUS, OTP, and DHCP servers used by the VPN gateways are deployed in a redundant fashion on different network subnets within the server module to ensure high availability and scalability of their respective services to the VPN clients tunnels.

Alternatives

An organization can further its security posture by deploying a network-based IDS (NIDS) and firewalling behind the VPN gateways before wireless user traffic hits the production wired network. This setup allows the network to audit, inspect, and filter user traffic that is being sent from the wireless clients to the enterprise network as defined by an organization's security policy. After providing the device and user authentication, the VPN gateway can optionally provide user authorization rights based on the group with which the wireless user is associated. All these security improvements are strongly recommended if the VPN user authentication policy chooses not to use OTP.

Also, a network designer looking for more security than the discussed design provides should consider the benefits of building a physically separate infrastructure for WLAN access. Physically separate Layer 2 and 3 segments on dedicated networking hardware are used to totally isolate the untrusted WLAN until traffic is decrypted at the VPN gateways and routed into the production wired network.

Additionally, the ability to have multiple SSIDs and VLANs on the access point allows the network designer to create a guest VLAN in order to allow guests of the enterprise access to the corporate network to gain access to a limited set of resources or VPN across the Internet to gain access to the guest's corporate network. In either of these cases, it is recommended that the network designer implement packet filters on the access and Layer 3 building distribution switch (or wherever the guest VLAN is terminated) to allow only traffic that conforms to the enterprise guest security policy. Similarly, a VLAN can be created for traditional wireless devices that support only static WEP, and an appropriate security policy can be enforced for this VLAN as well. Refer to Appendix A for an example of implementation of VPN design with the use of VLANs on the access points (large-enterprise VPN design).

Medium WLAN Design

The medium network WLAN overlays wireless on top of the campus portion of the SAFE medium network design. All the components for implementing the mitigation techniques are contained within the medium-campus module. These components are intended to allow WLAN access for end users within the medium-network campus. Specifics for implementing each mitigation technique are discussed in detail in the following section.

Design Guidelines

In the medium WLAN design, it is assumed that all WLAN devices are connected to a single IP subnet to enable end-user mobility throughout the medium WLAN design. An assumption is made in the designs that most services available to the medium wired network are also available to the medium WLAN design. Keeping with the design foundation for the SAFE medium network, the medium WLAN design does not offer high availability. Both EAP and VPN are considered viable security options for a medium WLAN design. Key devices for both the EAP and VPN options are supported in the campus module of the SAFE medium network design. For both options, network designers should give special consideration to the location of the RADIUS and DHCP servers used by the EAP and VPN WLAN solutions. The location of the servers will depend on the type of office the medium-network WLAN represents, medium business or branch office. If the medium network is the main business office, the DHCP and RADIUS servers will be located on the local network. If the medium network is a branch office, the DHCP and RADIUS servers might reside at the corporate office, with connectivity via the WAN module or through a VPN in the corporate Internet module. If the DHCP and RADIUS servers are located at the corporate office, wireless users will be denied access to the local network if the access point or VPN gateways cannot communicate with the RADIUS server for any reason, such as loss of WAN connectivity. Also, if the DHCP servers are unavailable to the medium network, the wireless clients will not be able to establish IP connectivity with the campus network. Security in the design is maintained by preventing network access if the RADIUS service fails. Because most of the mitigation against security risks relies on the RADIUS service, this behavior is required. Overall, management of the solution is hindered if DHCP services fail. Specifics for accomplishing these goals are detailed within each mitigation techniques section.

Network Management

In order to isolate management traffic from user traffic, it is recommended to use VLANs on the access points. Creating a management VLAN on the access point and restricting access to the access point via the management subnet by implementing ACLs in the building distribution Layer 3 switch is recommended. The ACLs should be specific to the IP address and protocols that the centralized multidevice access point configuration tool require. Note that because access points support only one wired interface, all management was done in band, versus the out-of-band management as recommended by SAFE enterprise. This setup contains a security risk because some

management traffic (SNMP, TFTP) must be sent in the clear in order to manage each access point via a central management station. The access point should be configured to provide central AAA of access point administrators via RADIUS or TACACS+, depending on the support of the deployed access points. Finally, network administrators should utilize a secure management transport such as SSH in order to manage the access points from the command line.

EAP with TKIP Option

Figure 10
Medium-Network EAP WLAN Design
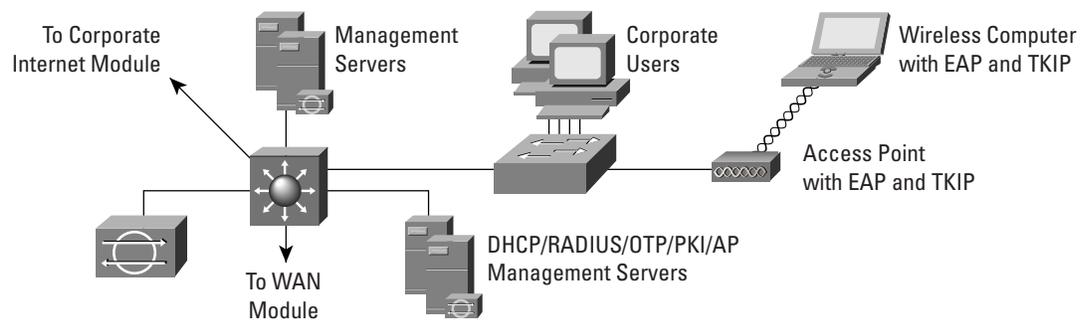
EAP access in the medium WLAN design has wireless access points connected to the existing Layer 2 access switch in the medium-campus module. RADIUS and DHCP servers are also located in the campus module, but off a distinct Layer 3 subnet on the central-campus Layer 3 switch. The wireless EAP users will require DHCP and RADIUS authentication services to access the medium-campus network. If the medium network is a branch office, the DHCP and RADIUS servers may reside at the corporate office.

The process of accessing the medium network is the same as that outlined in the standard medium WLAN design guidelines.

Alternatives

In the case of a branch office where RADIUS and DHCP servers reside at the corporate office, RADIUS and DHCP server redundancy need to be considered. As an alternative, the network designer could choose to implement local RADIUS and DHCP servers to provide WLAN access in the event of WAN link connectivity failure to the corporate network. If this alternative is chosen, the network designer needs to consider administration and maintenance of multiple (or hundreds in the case of a retail network) RADIUS and DHCP servers.

As discussed in the Large-Enterprise EAP design guidelines section, EAP design along with VLANs on access points enables the network designer to implement user differentiation (using wired and wireless VLANs) and enforce VLAN assignment for users and user groups using the RADIUS server. Furthermore, appropriate Layer 3 filters can be enforced at the access and distribution layer for each user group.

IPsec VPN Option

Figure 11

Medium Network VPN WLAN Design
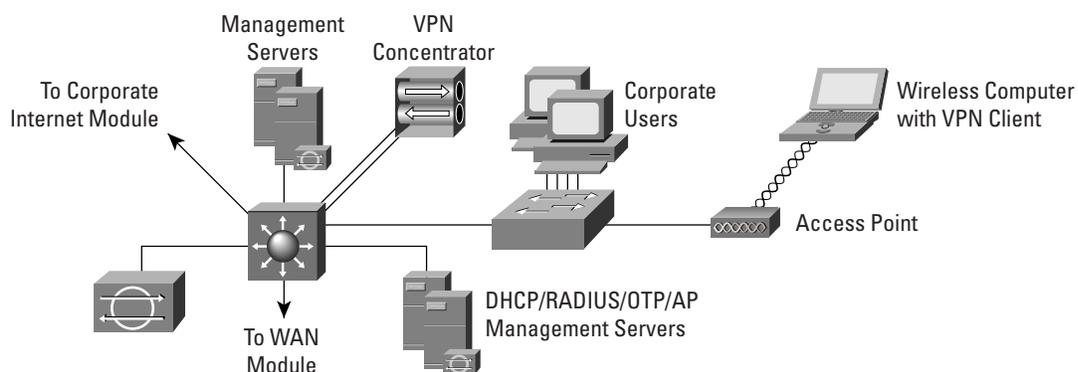
The IPsec VPN option in the medium network is very similar to the VPN option for the large WLAN design. The primary differences are in the physical connectivity of the VPN gateway that divides the wireless network from the wired network. The VPN gateway connects its interfaces to the campus-module Layer 3 switch using two different VLANs. It should be noted that this recommendation is in direct conflict with the "Switches Are Targets" axiom in the core SAFE security documents. When you use VLANs in a security role, you are effectively extending the security perimeter to include the switch itself. A compromise of the switch allows the hacker to bypass the VPN concentrator. This VLAN-based option was chosen because the alternative was not financially viable for businesses likely to deploy a midsize network. See the following alternatives for a more secure option using additional equipment.

The VPN gateway connects its public interface to one VLAN that can connect to the wireless access points. As in the standard VPN WLAN design, it is recommended that the VPN concentrator perform DHCP relay between the public side and the private side of the concentrator. This allows the network designer to more effectively deploy and manage the DHCP services for the WLAN. The private interface of the VPN gateway connects to a VLAN with access to the wired network. The wireless access points connect to existing Layer 2 switches in the campus-module access layer on a dedicated VLAN and forward traffic from the WLAN to the VLAN with VPN connectivity. Like the large WLAN and general VPN WLAN design, the access and building distribution module Layer 3 switches are configured with ACLs to permit only protocols necessary for VPN connectivity and management.

The wireless client establishes an IPsec connection to the wireless VPN gateway. In the process of doing so, the VPN gateway provides device and user authentication via the IPsec VPN. The VPN gateway can use digital certificates or preshared keys for wireless client device authentication. The VPN end user employs OTPs to authenticate to the VPN gateway. The VPN gateway uses RADIUS services, which in turn contact the OTP server for user authentication. The VPN gateway uses DHCP for IP addressing information in order for the WLAN client to communicate through the VPN tunnel.

Alternatives

An organization can further its security posture by deploying NIDS and firewalling behind the VPN gateways before wireless user traffic hits the production wired network. This setup allows the network to audit, inspect, and filter user traffic that is being sent from the wireless clients to the medium network as defined by an organization's security policy. Both of these security improvements are strongly recommended if the VPN user authentication policy chooses not to use OTP.

Also, a network designer looking for more security than these designs provide should consider the benefits of a design similar to the standard VPN WLAN option. A design specific to the medium WLAN is depicted in Figure 12. The primary benefit is the clear delineation between the public and private interfaces of the VPN gateway. The primary detraction from this design is the potentially high cost of deploying additional Layer 2 switches just to connect the wireless access points. New features in VPN concentrators allow the concentrator to provide DHCP relay services to a DHCP server behind the VPN concentrator. This deployment option does open the DHCP server to the security risks outlined in the standard VPN design, but is recommended rather than deploying a DHCP server outside the VPN concentrator.

Figure 12
Medium-Network VPN WLAN Design
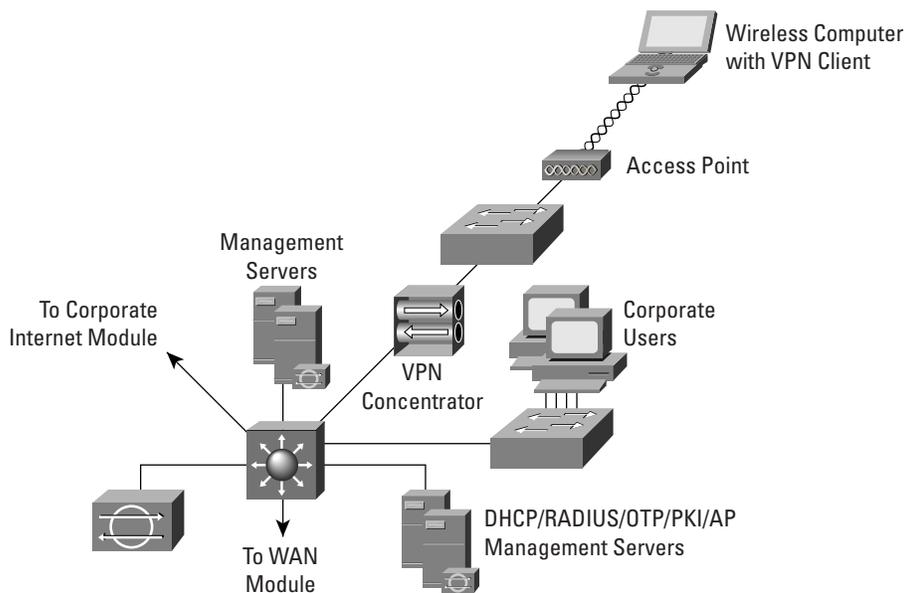
Small WLAN Design

The small WLAN design overlays WLAN on top of the SAFE small network design. The small WLAN design is contained within the campus module. This section discusses one option, EAP with TKIP, for providing WLAN users connectivity to the wired campus. IPsec is not presented as an option because of the financial burden of implementing a dedicated WLAN VPN in a network of this size.

Design Guidelines

The following sections detail the small WLAN design. Because the small-network design has a single Layer 2 switch for its campus connectivity (as shown in Figure 13), all devices are assumed to have a single IP subnet network to enable access point roaming.

Network Management

Network management traffic from the management hosts to the access points is unrestricted because of the lack of a Layer 3 device in the small campus. Some management traffic is sent in the clear to each access point, as is done for the rest of the SAFE small design.

EAP with TKIP Option

Figure 13
Small-Network EAP WLAN Design
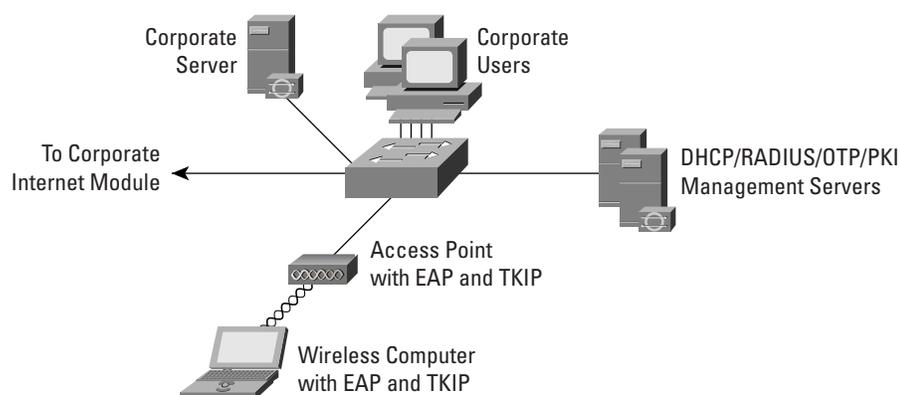
Cisco EAP access in the small WLAN design has wireless access points connected to the existing Layer 2 access switch in the small-campus module. The wireless EAP users require DHCP and RADIUS authentication services to access the small-campus network. Because of the single-site nature of small networks, the RADIUS and DHCP servers reside locally connected to the Layer 2 switch in the campus module.

The process of accessing the small network is the same as that outlined in the standard WLAN design guidelines.

Alternatives

Although not recommended, if an organization is comfortable with managing the key distribution issues, static WEP (with the cryptography fixes listed earlier) can be used as an alternative to EAP.

Remote WLAN Design

The remote WLAN design shows remote wireless solutions for the two primary types of remote VPN connectivity defined by SAFE: software-based VPNs and hardware-based VPNs. This section discusses these two options for providing WLAN users connectivity to a central office (small, medium, or enterprise) within the SAFE design.

Software VPN Remote WLAN Design
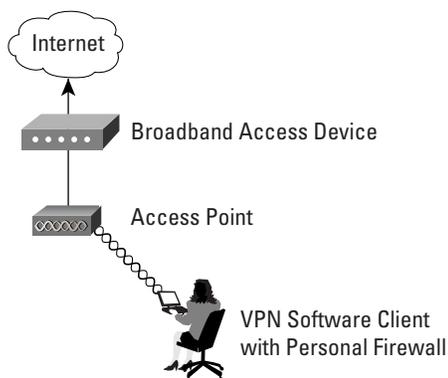
The IPsec VPN option in the remote network is recommended when the wireless user requires security from the wireless device to the corporate network (as illustrated in Figure 14). This is the most common configuration for remote workers who may not have IT-managed hardware resources at their remote location. Part-time teleworkers fall into this category. The access point can be set up with almost any configuration that allows connectivity to the broadband device because the security is handled via the VPN client with personal firewall software. In addition, network designers can consider putting filters on the access point to allow only IPsec, DHCP, and DNS traffic in order to mitigate attacks from the WLAN to the wired LAN. The access point filters are detailed in Appendix A, "Validation Lab."

Hardware VPN Remote WLAN Design
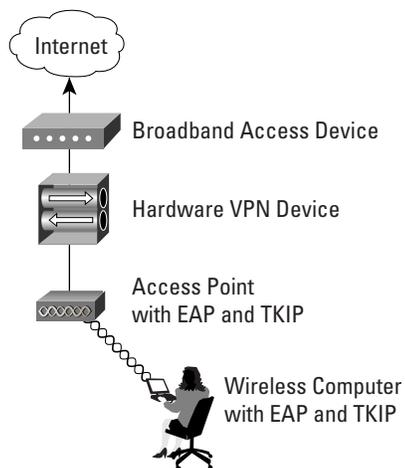
For configurations where an organization's IT department manages VPN and wireless gear at a user's remote location, using EAP from the PC to the access point and then IPsec from the hardware VPN device to the central office provides a robust security solution for a remote worker (as illustrated in Figure 15). Full-time teleworkers are the individuals most likely to take advantage of this configuration. When the remote location is using a hardware VPN and EAP for wireless, the design is nearly identical to that of the small WLAN design. Remember that the same caveats regarding RADIUS access apply. Wireless users are denied access to the local network if the access point cannot communicate with the RADIUS server for any reason, such as loss of IPsec VPN connectivity. This design also requires that the remote network have a unique IP range to facilitate IT management of the remote access point. If the hardware device uses Network Address Translation (NAT) for all traffic from the remote site to one IP address, the IT department cannot manage the access point.

Appendix A: Validation Lab

A reference Cisco SAFE Blueprint for network security wireless LAN (WLAN) implementation exists to validate the functionality described in this document. This appendix details the configurations of the specific devices as they relate to WLAN functionality within each module, as well as the overall guidelines for general device configuration. The following are configuration snapshots from the live devices in the lab. Cisco does not recommend applying these configurations directly to a production network.

Overall Guidelines

The sample commands presented in this section correspond in part to the SAFE WLAN design guidelines presented earlier in this document.

SAFE WLAN Standard Configuration for Access Points

EAP Access Point

Figure A-1 shows the Authenticator Configuration window (under Setup >> Security section) on an access point configured to allow Extensible Authentication Protocol (EAP) wireless clients to be authenticated by a Remote Access Dial-In User Service (RADIUS) server. It is assumed that either the RADIUS server itself or a network OS server (such as a Windows NT server) contains a database of valid users along with passwords.

Figure A-1

Authenticator Configuration Window for an EAP Access Point

Figure A-2 illustrates the security configuration for an EAP access point. "Full Encryption" (wired equivalent privacy [WEP]) is mandated by the access point; in addition, the access point allows network EAP as the only authentication method. EAP types configured for this deployment included Cisco-EAP (LEAP), Protected EAP (PEAP), and EAP-Transport Layer Security (EAP-TLS).

Figure A-2

WEP Configuration for an EAP Access Point

VPN Access Point

As Figure A-3 illustrates, an access point is configured to allow open authentication, and WEP encryption is not enabled for virtual-private-network (VPN) wireless clients authenticating to a wired network.

Figure A-3
WEP Configuration for a VPN Access Point

The following sections detail sample configurations needed on access points to enable EAP or VPN (shown in screen captures) as detailed in the axioms and design guidelines sections of this document. The sample configuration screen captures were taken for the large-enterprise design.

As discussed in the design section of this document, a VPN access point should be configured with EtherType, protocol, and port filters based on a company's wireless usage policy. SAFE WLAN recommends restrictive filters that allow only the necessary protocols required for establishing a secure tunnel to a VPN gateway. The Internet Control Message Protocol (ICMP) IP protocol filter is allowed for troubleshooting purposes. Tables A-1 and A-2 list the inbound (receive) and outbound (transmit) filters to be set on the VPN access point radio interface:

Table A-1   VPN Access Point Radio Protocol Filters—Inbound (receive)

Filter Type	Protocol	Value	Disposition
EtherType	ARP	0x0806	Forward
EtherType	IP	0x0800	Forward
IP Protocol	UDP	17	Forward
IP Protocol	ESP	50	Forward
IP Protocol	ICMP	1	Forward
IP Port	BootPC	68	Forward
IP Port	DNS	53	Forward
IP Port	IKE	500	Forward

Table A-2   VPN Access Point Radio Protocol Filters—Outbound (transmit)

Filter Type	Protocol	Value	Disposition
EtherType	ARP	0x0806	Forward
EtherType	IP	0x0800	Forward
IP Protocol	UDP	17	Forward
IP Protocol	ESP	50	Forward
IP Protocol	ICMP	1	Forward
IP Port	BootPC	68	Forward
IP Port	DNS	53	Forward
IP Port	IKE	500	Forward

When creating these filter sets on VxWorks APs, be sure to:

- Set "Default Disposition" of the filter set to "block."
- Enable specific traffic types to flow by adding the specified values (in Table A-1 or A-2) to "Special Cases" and select "forward" as the disposition for each special case.
- After creating all the filter sets, be sure to apply them to the access point radio interface (or to the VPN virtual LAN [VLAN]).

SAFE Wireless LAN Standard Configuration for Clients

The following sections detail sample configurations needed for wireless clients to enable VPN or EAP (shown in screen captures) as detailed in axioms and design guidelines sections of this document. The sample configuration screen captures were taken for the large-enterprise design. However, configuration for a VPN wireless client (or a LEAP wireless client) is identical for all designs.

VPN Client

For a wireless user connecting to a wired network using a VPN client, encryption and authentication at the Layer 2 level are usually disabled. However, the IT administrator could choose to use static-WEP or Temporal Key Integrity Protocol (TKIP) or EAP with TKIP at the Layer 2 network level. Figures A-4 and A-5 illustrate the sample setup.

Figure A-4
System Parameters Configuration on a VPN Client
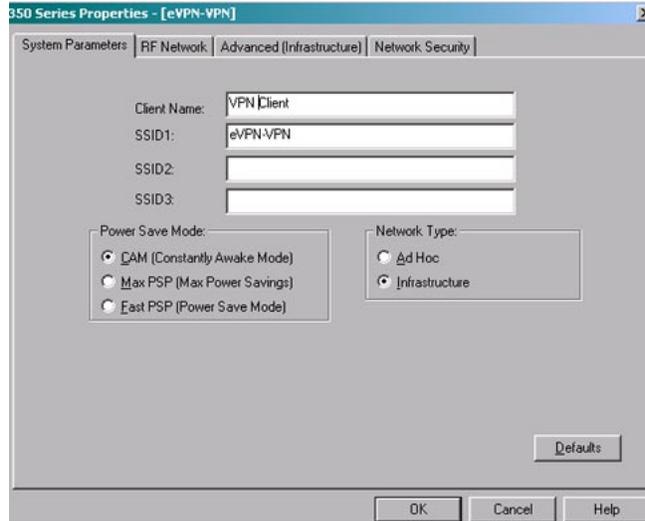
Figure A-5
Network Security Configuration on a VPN Client
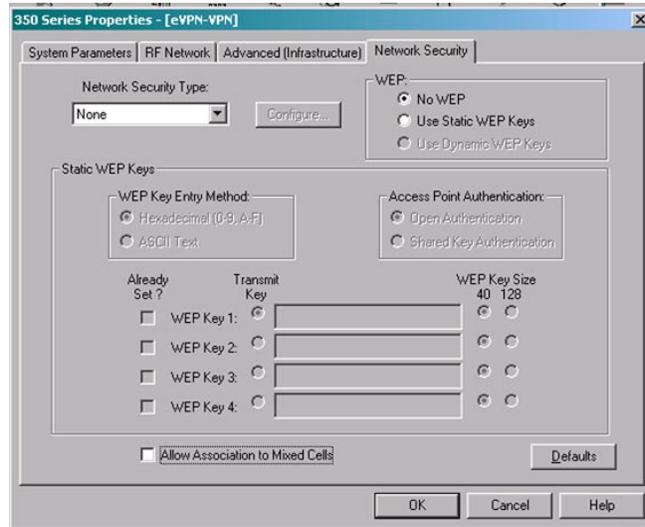
EAP Client

A wireless client is configured for EAP by specifying the appropriate service set ID (SSID) and security settings using the Cisco Aironet® Client utility. However, it should be noted that OS-level configuration is usually required for EAP-TLS and PEAP (for example, configuring a Microsoft Windows XP client with the appropriate EAP-TLS or PEAP settings). Figures A-6, A-7, and A-8 illustrate sample configuration for a LEAP client. Figures A-9 and A-10 illustrate sample configuration for an EAP-TLS or PEAP client.

Figure A-6
System Parameters Configuration for EAP Wireless Clients
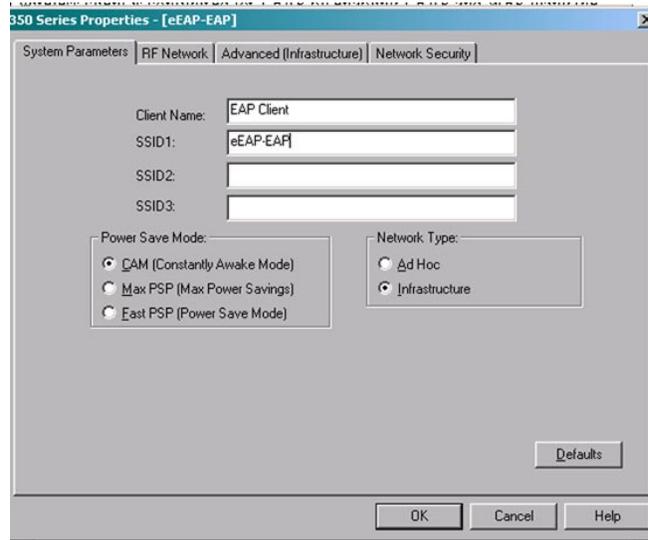
Figure A-7
Network Security Configuration for LEAP Wireless Clients
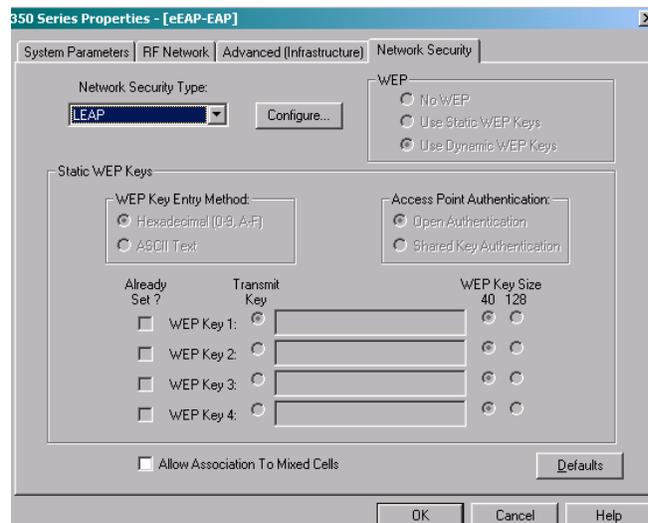
Figure A-8

LEAP Settings Configurations for LEAP Wireless Clients
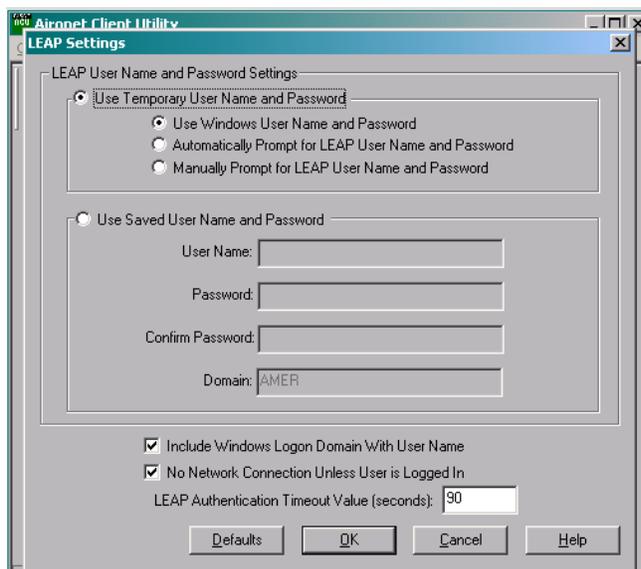
Figure A-9

Network Security Configuration for PEAP or EAP-TLS Wireless Clients
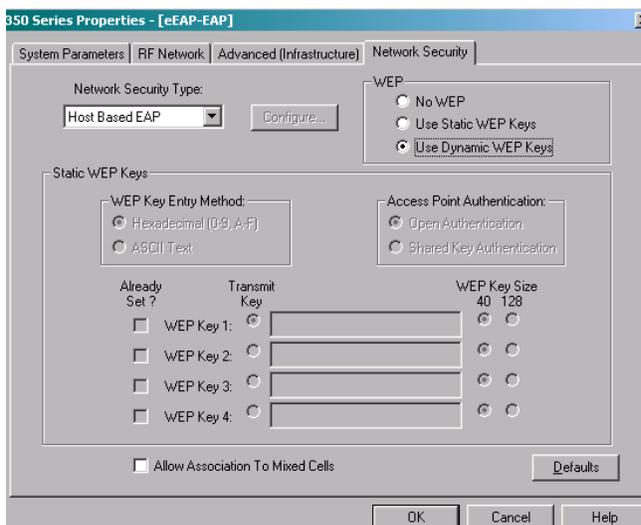
Figure A-10
Authentication Configuration for PEAP or EAP-TLS Wireless Clients for Windows
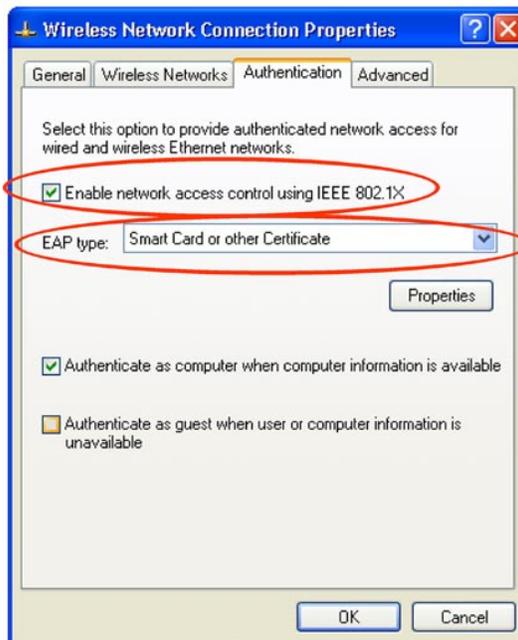
Large-Enterprise Design Module Configurations

This section details end-to-end EAP and VPN architecture configurations for a large-enterprise network design.

EAP with TKIP Architecture

The following shows a configuration snapshot from the SAFE large-enterprise EAP WLAN design. Figure A-11 illustrates the EAP design for a large-enterprise network.

Figure A-11

Large-Enterprise EAP WLAN Design
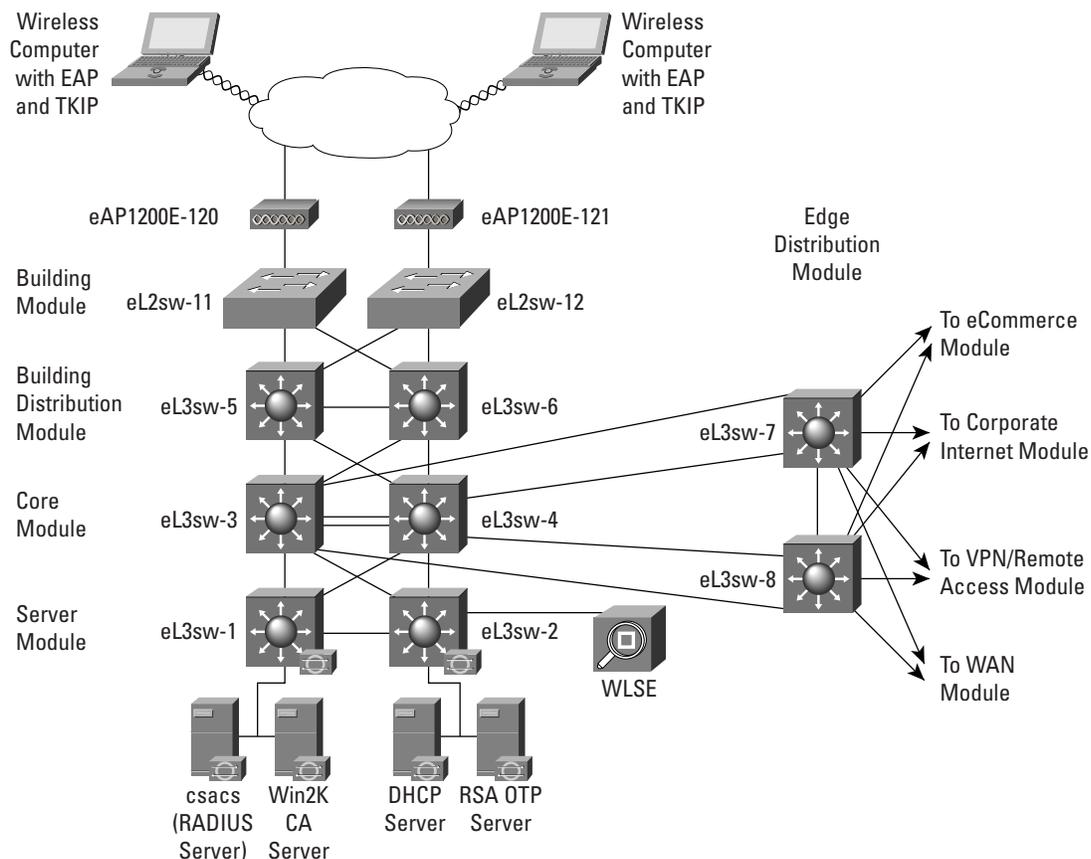
Products used include the following:

- Cisco Catalyst® 6506 Layer 3 switches (product numbers eL3sw-1 to eL3sw-8)

- Cisco Catalyst 4003 Layer 2 switches (product numbers eL2sw-11 to L2sw-12)

- Cisco Aironet 1200 access points and clients (product numbers eAP1200E-120 to eAP1200V-121 and wireless clients)

- Cisco Secure Access Control Server (ACS v3.1)

- Windows 2000 Dynamic Host Configuration Protocol (DHCP) server

- Windows 2000 certificate authority server

- RSA one-time-password (OTP) server

- Cisco Wireless LAN Solution Engine (WLSE)

The following sections discuss configurations specific to the SAFE WLAN large-network design. For generic configuration guidelines for a large enterprise network, refer to "Cisco SAFE: A Security Blueprint for Enterprise Networks."

Cisco Aironet 1200 Access Points (product numbers eAP1200E-120 to eAP1200E-121) and Wireless Clients:

Refer to the configuration samples in the "Overall Guidelines" section of this appendix for configuring Cisco Aironet access points and wireless clients for EAP. In the SAFE architecture lab, the large-enterprise EAP WLAN design was implemented with wireless VLANs. This section details the implementation details specific to VLAN implementation along with EAP WLAN design.

As Figures A-12 and A-13 illustrate, an access point is configured with multiple security profiles, which are correlated with SSID associations and VLAN IDs. An EAP authenticated user is configured for full 128-bit encryption.

Figure A-12
EAP Access Point VLAN Summary Page

As discussed in the design section, marketing and engineering VLANs were created to correspond with user groups on the Cisco Secure ACS server. Thus, when EAP wireless users associate, they are temporarily placed in VLAN 73, and the authentication request is sent to the ACS server. When the users have been authenticated based on the configured username, they are placed in the appropriate marketing or engineering VLAN. A management VLAN has also been created (VLAN 70) for access point management. Refer to the VLAN deployment guide on Cisco.com for more details:

http://www.cisco.com/en/US/products/hw/wireless/ps430/prod_technical_reference09186a00801444a1.html

In addition, an alternative configuration is to create guest (eEAP-Guest) and static WEP (eEAP-Static) SSIDs that are associated with separate VLANs and security profiles to differentiate user access.

Figure A-13
EAP Access Point Service Set Summary Page

Cisco Catalyst 6506 Layer 3 switches (product numbers eL3sw-5 and eL3sw-6) (WLAN building module-to-building distribution module interconnection):

```
! Management VLAN for APs in the campus network
interface Vlan70
ip address 10.1.70.5 255.255.255.0
ip access-group 170 in
ip access-group 171 out
ip helper-address 10.1.11.50
no cdp enable

!EAP VLAN for authenticated users
interface Vlan73
ip address 10.1.73.5 255.255.255.0
ip access-group 172 in
ip access-group 173 out
ip helper-address 10.1.11.50
no cdp enable
```

The following are ACLs for the management VLAN (Interface 70):

```
! Permit only authentication and accounting requests from APs to RADIUS server on the management
VLAN
access-list 170 permit udp host 10.1.70.120 gt 1023 host 10.1.20.54 eq 1645
access-list 170 permit udp host 10.1.70.120 gt 1023 host 10.1.20.54 eq 1646
access-list 170 permit udp host 10.1.70.121 gt 1023 host 10.1.20.54 eq 1645
access-list 170 permit udp host 10.1.70.121 gt 1023 host 10.1.20.54 eq 1646

! Permit only SNMP and TFTP traffic from wireless APs to WLSE* in out of band management network
access-list 170 permit udp host 10.1.70.120 eq snmp host 10.1.20.150
access-list 170 permit udp host 10.1.70.121 eq snmp host 10.1.20.150
access-list 170 permit udp host 10.1.70.120 host 10.1.20.150 eq tftp
access-list 170 permit udp host 10.1.70.121 host 10.1.20.150 eq tftp

! Permit outgoing traffic for AP web management in the out of band management network
access-list 170 permit tcp host 10.1.70.120 eq www 10.1.20.0 0.0.0.255 gt 1023 established
access-list 170 permit tcp host 10.1.70.121 eq www 10.1.20.0 0.0.0.255 gt 1023 established

!Permit SSH traffic from the APs to out of band management network
access-list 170 permit tcp host 10.1.70.120 eq 22 10.1.20.0 0.0.0.255 gt 1023 established
access-list 170 permit tcp host 10.1.70.121 eq 22 10.1.20.0 0.0.0.255 gt 1023 established
```

```
! Permit only BOOTP requests to pass through to DHCP server
access-list 170 permit udp host 0.0.0.0 eq bootpc host 255.255.255.255 eq bootps

! Deny all other traffic
access-list 170 deny ip any any log

! Permit only SNMP and TFTP traffic from WLSE* to APs in out of band management network
access-list 171 permit udp host 10.1.20.150 gt 1023 host 10.1.70.120 eq snmp
access-list 171 permit udp host 10.1.20.150 gt 1023 host 10.1.70.121 eq snmp
access-list 171 permit udp host 10.1.20.150 gt 1023 host 10.1.70.120 eq tftp
access-list 171 permit udp host 10.1.20.150 gt 1023 host 10.1.70.121 eq tftp

! Permit outgoing web traffic from out of band network to APs for management
access-list 171 permit tcp 10.1.20.0 0 .0.0.255 gt 1023 host 10.1.70.120 eq www
access-list 171 permit tcp 10.1.20.0 0.0.0.255 gt 1023 host 10.1.70.121 eq www
access-list 171 permit tcp 10.1.20.0 0.0.0.255 gt 1023 host 10.1.70.120 eq 22
access-list 171 permit tcp 10.1.20.0 0.0.0.255 gt 1023 host 10.1.70.121 eq 22

! Permit RADIUS responses from AAA Server
access-list 171 permit udp host 10.1.20.54 eq 1645 host 10.1.70.120 gt 1023
access-list 171 permit udp host 10.1.20.54 eq 1646 host 10.1.70.120 gt 1023
access-list 171 permit udp host 10.1.20.54 eq 1645 host 10.1.70.121 gt 1023
access-list 171 permit udp host 10.1.20.54 eq 1646 host 10.1.70.121 gt 1023

! Deny all other IP traffic to APs
access-list 171 deny ip any host 10.1.70.120 log
access-list 171 deny ip any host 10.1.70.121 log
access-list 171 deny ip any any log
```

The following are ACLs for the EAP VLAN (Interface 73):

```
!Deny user access to APs management VLAN
access-list 172 deny ip 10.1.73.0 0.0.0.255 10.1.70.0 0.0.0.255 log
! Permit all IP traffic from EAP VLAN in wireless network to any destination
access-list 172 permit ip 10.1.73.0 0.0.0.255 any
! Permit only BOOTP requests to pass through to DHCP server
access-list 172 permit udp host 0.0.0.0 eq bootpc host 255.255.255.255 eq bootps
!Deny all other traffic
access-list 172 deny ip any any log
```

```
! Permit all IP traffic from any destination to EAP VLAN in wireless network
access-list 173 permit ip any 10.1.73.0 0.0.0.255
!Deny all other traffic
access-list 173 deny ip any any log
```

VPN Architecture

The following shows a configuration snapshot from the SAFE large-enterprise VPN WLAN design. Figure A-14 illustrates the VPN design for a WLAN in a large enterprise.

Figure A-14
Large-Enterprise VPN WLAN Design
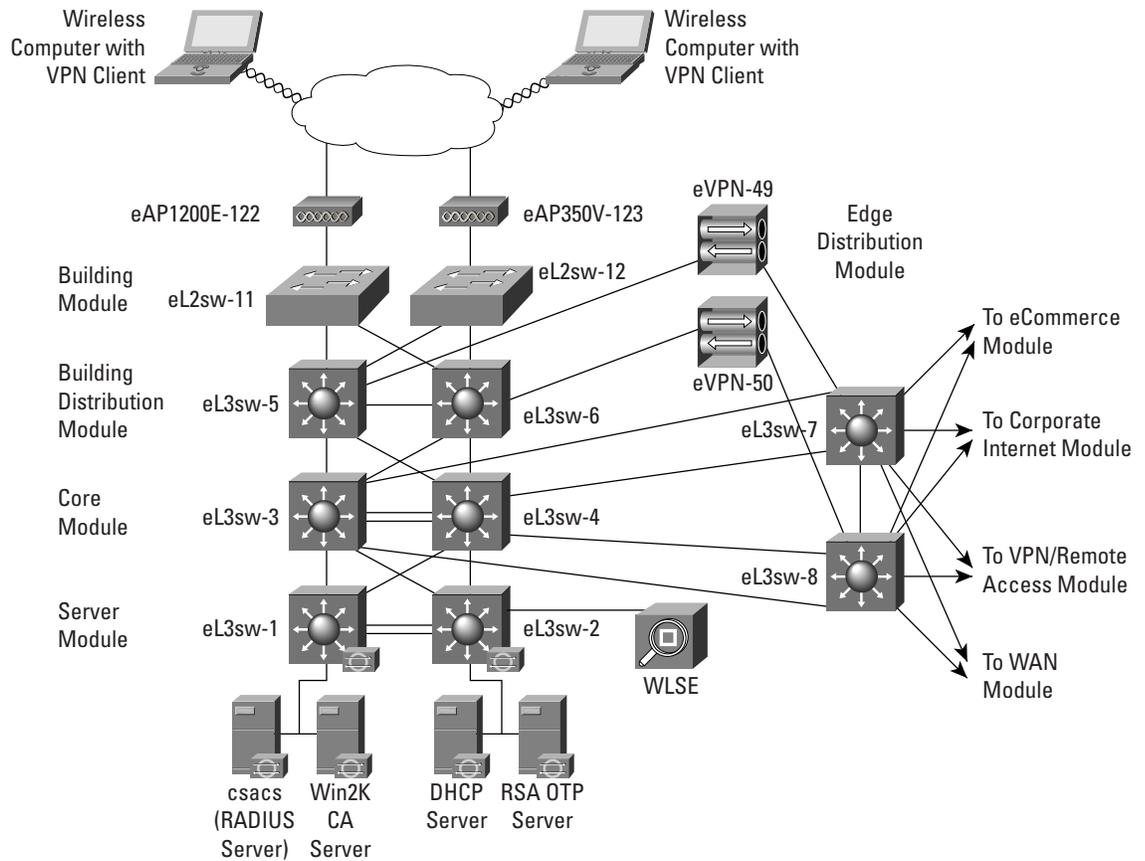
Products used include the following:

- Cisco Catalyst 6506 Layer 3 switches (product numbers eL3sw-1 to eL3sw-8)
- Cisco Catalyst 4003 Layer 2 switches (product numbers eL2sw-9 to eL2sw-14)
- Cisco VPN 3015 Concentrator (product numbers eVPN-49 to 50)
- Cisco Aironet 1200 access points and clients (product numbers eAP1200V-120 to eAP350V-121 and wireless clients)

- Cisco Secure Access Control Server (ACS v3.1)
- Windows 2000 DHCP server
- Cisco Intrusion Detection System (IDS) Host Sensor
- Windows 2000 certificate authority server
- RSA OTP server
- Cisco Wireless LAN Solution Engine

The following sections discuss conf igurations specific to the SAFE WLAN large-enterprise VPN network design. For generic configuration guidelines for a large-enterprise network, refer to "Cisco SAFE: A Security Blueprint for Enterprise Networks."

Cisco Aironet 1200 Access Points (product numbers eAP1200V-120 and eAP350V-121) and Wireless Clients:

Refer to the configuration samples in the "Overall Guidelines" section of this appendix for configuring Cisco Aironet access points and wireless clients for VPN connectivity over a WLAN. In the SAFE architecture lab, the large-enterprise VPN WLAN design was implemented with wireless VLANs. This section details the implementation details specific to VLAN implementation along with the VPN-over-WLAN design.

As Figure A-15 illustrates, an access point is configured with multiple security profiles, which are correlated with SSID associations and VLAN IDs. As stated in the "Standard VPN design guidelines" section, Layer 2 encryption and authentication is usually disabled for IP security (IPsec) VPN-over-WLAN deployments. However, if the IT administrator wishes, Layer 2 encryption and authentication can be optionally enabled. In the SAFE architecture lab, the large VPN design was implemented with Layer 2 encryption enabled. A VPN user is configured to have full 128-bit WEP encryption with Cisco TKIP and message integrity check (MIC) enabled.

Figure A-15
VPN Access Point VLAN Summary Page

As discussed in the design section, VPN users can be placed in a separate VLAN based on the SSID with which they are associated. A management VLAN has also been created (VLAN 80) for access point management. Refer to the VLAN deployment guide on Cisco.com for more details:

http://www.cisco.com/en/US/products/hw/wireless/ps430/prod_technical_reference09186a00801444a1.html

In addition, an alternative configuration is to create guest (eVPN-Guest) and static WEP (eVPN-Static) SSIDs that are associated with separate VLANs and security profiles to differentiate user access (as shown in Figure A-16).

Figure A-16
VPN Access Point Service Set Summary Page

Cisco Catalyst 6506 Layer 3 Switches (product numbers eL3sw-5 and eL3sw-6) (WLAN building module-to-building distribution module interconnection):

```
! Management VLAN for APs in the campus network
interface Vlan80
ip address 10.1.80.5 255.255.255.0
ip access-group 180 in
ip access-group 181 out
ip helper-address 10.1.11.50
no cdp enable

! VLAN for VPN users
interface Vlan83
ip address 10.1.83.5 255.255.255.0
ip access-group 182 in
ip access-group 183 out
ip helper-address 10.1.11.50
no cdp enable
```

!The following are ACLs for the management VLAN (Interface 80):

```
! Permit only authentication and accounting requests from AP to RADIUS server
access-list 180 permit udp host 10.1.80.122 gt 1023 host 10.1.20.54 eq 1645
access-list 180 permit udp host 10.1.80.122 gt 1023 host 10.1.20.54 eq 1646
access-list 180 permit udp host 10.1.80.123 gt 1023 host 10.1.20.54 eq 1645
access-list 180 permit udp host 10.1.80.123 gt 1023 host 10.1.20.54 eq 1646

! Permit only SNMP and TFTP traffic from wireless APs to WLSE* in out of band management network
access-list 180 permit udp host 10.1.80.122 eq snmp host 10.1.20.150
access-list 180 permit udp host 10.1.80.123 eq snmp host 10.1.20.150
access-list 180 permit udp host 10.1.80.122 host 10.1.20.150 eq tftp
access-list 180 permit udp host 10.1.80.123 host 10.1.20.150 eq tftp
```

```
! Permit outgoing web management traffic from AP to out of band management network
access-list 180 permit tcp host 10.1.80.122 eq www 10.1.20.0 0.0.0.255 gt 1023 established
access-list 180 permit tcp host 10.1.80.123 eq www 10.1.20.0 0.0.0.255 gt 1023 established

!Permit SSH traffic from the APs to out of band management network
access-list 180 permit tcp host 10.1.80.122 eq 22 10.1.20.0 0.0.0.255 gt 1023 established
access-list 180 permit tcp host 10.1.80.123 eq 22 10.1.20.0 0.0.0.255 gt 1023 established

! Deny all other traffic
access-list 180 deny ip any any log

! Permit incoming web traffic from out of band management network to APs
access-list 181 permit tcp 10.1.20.0 0.0.0.255 gt 1023 host 10.1.80.122 eq www
access-list 181 permit tcp 10.1.20.0 0.0.0.255 gt 1023 host 10.1.80.123 eq www
access-list 181 permit tcp 10.1.20.0 0.0.0.255 gt 1023 host 10.1.80.122 eq 22
access-list 181 permit tcp 10.1.20.0 0.0.0.255 gt 1023 host 10.1.80.123 eq 22

! Permit only SNMP and TFTP traffic from WLSE to wireless APs
access-list 181 permit udp host 10.1.20.150 gt 1023 host 10.1.80.122 eq snmp
access-list 181 permit udp host 10.1.20.150 gt 1023 host 10.1.80.123 eq snmp
access-list 181 permit udp host 10.1.20.150 gt 1023 host 10.1.80.122 eq tftp
access-list 181 permit udp host 10.1.20.150 gt 1023 host 10.1.80.123 eq tftp

! Permit RADIUS responses from AAA Server to APs
access-list 181 permit udp host 10.1.20.54 eq 1645 host 10.1.80.122 gt 1023
access-list 181 permit udp host 10.1.20.54 eq 1645 host 10.1.80.123 gt 1023
access-list 181 permit udp host 10.1.20.54 eq 1646 host 10.1.80.122 gt 1023
access-list 181 permit udp host 10.1.20.54 eq 1646 host 10.1.80.123 gt 1023

! Deny all other IP traffic to APs
access-list 181 deny ip any host 10.1.80.122 log
access-list 181 deny ip any host 10.1.80.123 log
access-list 181 deny ip any any log
```

!The following are ACLs for the VPN VLAN (Interface 83):

```
! Permit IPsec traffic to VPN gateway subnet
access-list 182 permit esp 10.1.83.0 0.0.0.255 10.1.50.0 0.0.0.255
access-list 182 permit udp 10.1.83.0 0.0.0.255 eq isakmp 10.1.50.0 0.0.0.255 eq isakmp

! Permit full ICMP for troubleshooting
access-list 182 permit icmp 10.1.83.0 0.0.0.255 10.1.50.0 0.0.0.255

! Permit DHCP requests for initial IP assignment for wireless client
access-list 182 permit udp host 0.0.0.0 eq bootpc host 255.255.255.255 eq bootps
access-list 182 permit udp 10.1.83.0 0.0.0.255 eq bootpc host 255.255.255.255 eq bootps
access-list 182 permit udp 10.1.83.0 0.0.0.255 eq bootpc host 10.1.11.50 eq bootps

! Deny all other traffic, don't log Windows file share broadcasts
access-list 182 deny udp 10.1.83.0 0.0.0.255 any eq netbios-ns
access-list 182 deny udp 10.1.83.0 0.0.0.255 any eq netbios-dgm
access-list 182 deny ip any any log

! Permit IPsec traffic from VPN gateway subnet to wireless subnet
access-list 183 permit esp 10.1.50.0 0.0.0.255 10.1.83.0 0.0.0.255
access-list 183 permit udp 10.1.50.0 0.0.0.255 eq isakmp 10.1.83.0 0.0.0.255 eq isakmp

! Permit Full ICMP for troubleshooting
access-list 183 permit icmp 10.1.50.0 0.0.0.255 10.1.83.0 0.0.0.255

! Permit DHCP responses for the initial IP assignment for the wireless client
access-list 183 permit udp host 10.1.11.50 eq bootps host 255.255.255.255 eq bootpc
access-list 183 permit udp host 10.1.11.50 eq bootps 10.1.83.0 0.0.0.255 eq bootpc

! Deny all other traffic
access-list 183 deny ip any any log
```

*Cisco Wireless LAN Solution Engine (WLSE) is a wireless network management appliance that enables configuration and management of a wireless LAN of up to 500 access points per device. Cisco WLSE was incorporated in the SAFE design for ease of configuration and management of all access points.

Cisco WLSE configuration details are as follows:

```
admin@wlse_safe:show config
hostname wlse_safe
interface ethernet0 192.168.253.150 255.255.255.0 default-gateway 192.168.253.57 up
ip domain-name safe-enterprise.com
ip name-server 10.1.11.50
!
snmp-server configuration:
RW community string: private
RO community string: public
!
telnet disabled
CLI auth: local
HTTP auth: local

admin@wlse_safe:show cdp run
!
CDP protocol is enabled...
broadcasting interval is every 60 seconds.
time-to-live of cdp packets is 180 seconds.
```

Please note that the Cisco Discovery Protocol was enabled because it is part of the out-of-band management network.

Medium Network Configurations

This section details end-to-end EAP and VPN architecture configurations for a medium-enterprise network.

EAP with TKIP Architecture

The following shows a configuration snapshot from the Cisco SAFE medium-enterprise WLAN design with EAP option. Figure A-17 illustrates the EAP WLAN design for a medium-enterprise network.

Figure A-17

Medium-Enterprise EAP WLAN Design
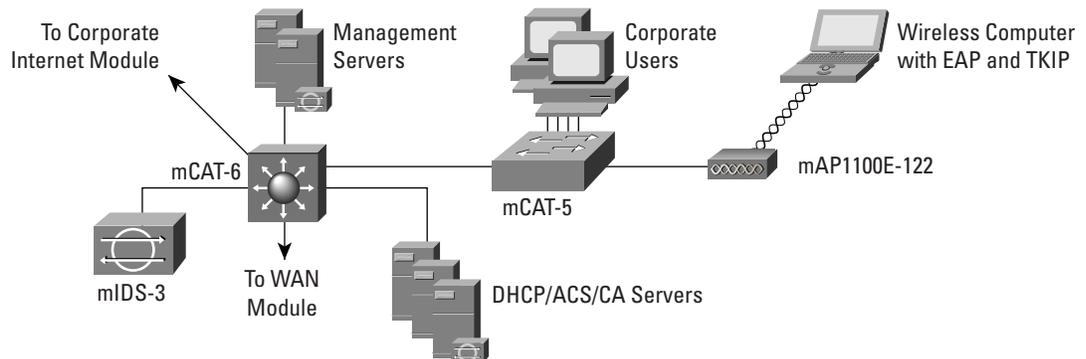
Products used include the following:

- Cisco Catalyst Layer 3 switch (product number mCAT-6)
- Cisco Catalyst Layer 2 switch (product number mCAT-5)
- Cisco Aironet access point and client (product number mAP1100E-122) and wireless client
- Cisco Secure Access Control Server (ACS v3.1)
- Windows 2000 DHCP server

The following sections discuss configurations specific to SAFE WLAN medium-network design (with EAP option). For generic configuration guidelines for a medium-enterprise network, refer to "SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks."

Cisco Aironet Access Point and Client (product number mAP1100E-122) and Wireless Client:

Refer to the configuration samples in the "Overall Guidelines" section of this appendix for configuring access points and wireless clients for the EAP option. In the SAFE architecture lab, the medium-enterprise EAP WLAN design was implemented with wireless VLANs. This section details the implementation details specific to VLAN implementation along with the EAP WLAN design.

mAP1100E-122 (AP1100) CLI Output:

```
MAP1100E-120#sh run
!
ssid mEAP-EAP
vlan 73
authentication open eap eap_methods
authentication network-eap eap_methods
accounting acct_methods
!
ssid mEAP-Guest
vlan 71
authentication open
accounting acct_methods
guest-mode
!
ssid mEAP-Static
vlan 72
authentication open
accounting acct_methods
!
interface Dot11Radio0.73
encapsulation dot1Q 73
no ip route-cache
no cdp enable
bridge-group 73
```

```
bridge-group 73 subscriber-loop-control
bridge-group 73 block-unknown-source
no bridge-group 73 source-learning
no bridge-group 73 unicast-flooding
bridge-group 73 spanning-disabled
!
interface FastEthernet0.73
encapsulation dot1Q 73
no ip route-cache
no cdp enable
bridge-group 73
no bridge-group 73 source-learning
bridge-group 73 spanning-disabled
```

As shown in the output, the access points in the medium design were also configured with multiple SSIDs (product numbers mEAP-Guest, mEAP-Static, etc.) that were associated with specific VLANs and security profiles for user differentiation.

Cisco Catalyst 6506 Layer 3 Switches (product number MCAT-6):

```
! Management (default) VLAN of the APs
interface Vlan70
ip address 10.3.70.1 255.255.255.0
ip access-group 170 in
ip access-group 171 out
ip helper-address 10.3.2.50
no ip redirects
no cdp enable

!Permit only authentication and accounting requests from AP to RADIUS server
access-list 170 permit udp host 10.3.70.120 gt 1023 host 10.3.8.253 eq 1645
access-list 170 permit udp host 10.3.70.120 gt 1023 host 10.3.8.253 eq 1646

! Permit outgoing web and SSH management traffic from AP to the out of band management network
access-list 170 permit tcp host 10.3.70.120 eq www 10.3.8.0 0.0.0.255 gt 1023 established
access-list 170 permit tcp host 10.3.70.120 eq 22 10.3.8.0 0.0.0.255 gt 1023 established

!Deny all other traffic
access-list 170 deny ip any any log

! Permit inbound management traffic (both http and SSH) to the AP
access-list 171 permit tcp 10.3.8.0 0.0.0.255 gt 1023 host 10.3.70.120 eq www
access-list 171 permit tcp 10.3.8.0 0.0.0.255 gt 1023 host 10.3.70.120 eq 22
```

```
! Permit RADIUS responses from AAA Server to the AP
access-list 171 permit udp host 10.3.8.253 eq 1645 host 10.3.70.120 gt 1023
access-list 171 permit udp host 10.3.8.253 eq 1646 host 10.3.70.120 gt 1023

! EAP VLAN definition
interface Vlan73
ip address 10.3.73.1 255.255.255.0
ip access-group 172 in
ip access-group 173 out
ip helper-address 10.3.2.50
no ip redirects
no cdp enable

! Permit only BOOTP requests to pass through to DHCP server
access-list 172 permit udp host 0.0.0.0 eq bootpc host 255.255.255.255 eq bootps
!Deny access to the management VLAN of the AP from the EAP VLAN
access-list 172 deny  ip 10.3.73.0 0.0.0.255 10.3.70.0 0.0.0.255 log
! Permit all IP traffic from any destination to EAP VLAN in wireless network
access-list 172 permit ip 10.3.73.0 0.0.0.255 any
!Deny all other traffic
access-list 172 deny    ip any any log

! Permit DHCP responses for the initial IP assignment for the wireless client
access-list 173 permit udp host 10.3.2.50 eq bootps host 255.255.255.255 eq bootpc
! Permit all IP traffic from any destination to EAP VLAN in wireless network
access-list 173 permit ip any 10.3.73.0 0.0.0.255
!Deny all other traffic
access-list 173 deny    ip any any log
```
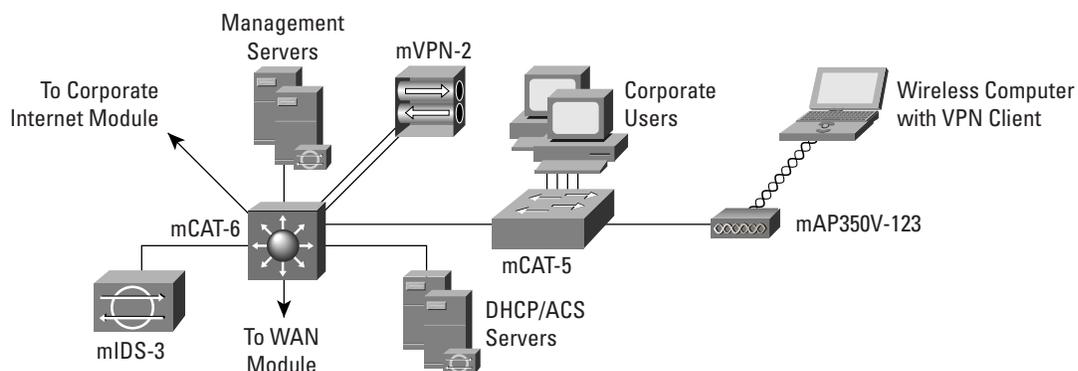
VPN Architecture

The following shows a configuration snapshot from the SAFE medium WLAN design with VPN option. Figure A-18 illustrates the VPN WLAN design for a medium network.

Figure A-18

Medium-Enterprise VPN WLAN Design

Products used include the following:

Cisco Catalyst Layer 3 switch (product number mCAT-6)

Cisco Catalyst Layer 2 switch (product number mCAT-5)

Cisco Aironet access point and client (product number mAP350V-123) and wireless client

Cisco VPN 3000 Series concentrator (product number mVPN-2)

Cisco Secure Access Control Server (ACS v3.1)

Windows 2000 DHCP server

Cisco IDS Host Sensor

Cisco Aironet Access Point (product number mAP350V-123) and Wireless Client:

Refer to the configuration samples in the "Overall Guidelines" section of this appendix for configuring access points and wireless clients for the VPN option.

**Cisco VPN 3000 Series Concentrator (product number mVPN-2):**

Cisco VPN 3000 Series concentrator (product number mVPN-2) was configured as follows: The public interface was on the same VLAN as the VPN user VLAN (mVPN-VPN), the private interface was on a separate VLAN, and the VPN concentrator was configured with DHCP relay enabled to forward DHCP requests from WLAN clients to the DHCP server in the wireless network. Thus, the Catalyst Layer-3 switch (product number MCAT-6) does not require any Layer 3 configurations. Figures A-19 and A-20 below illustrate the VPN concentrator configuration.

Figure A-19

VPN Concentrator Configuration
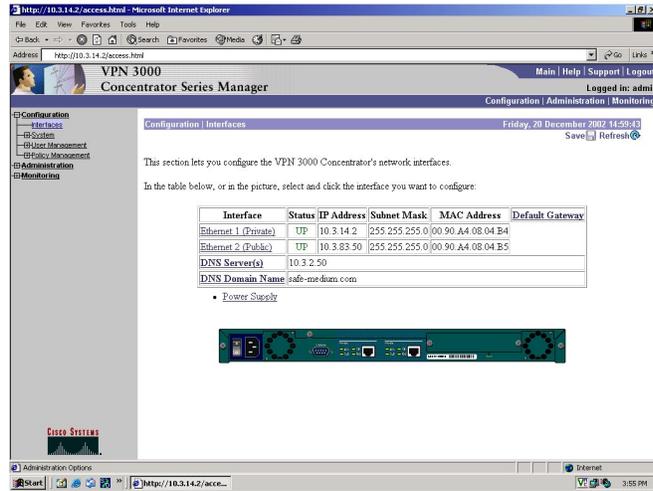
Figure A-20

VPN Concentrator Configuration
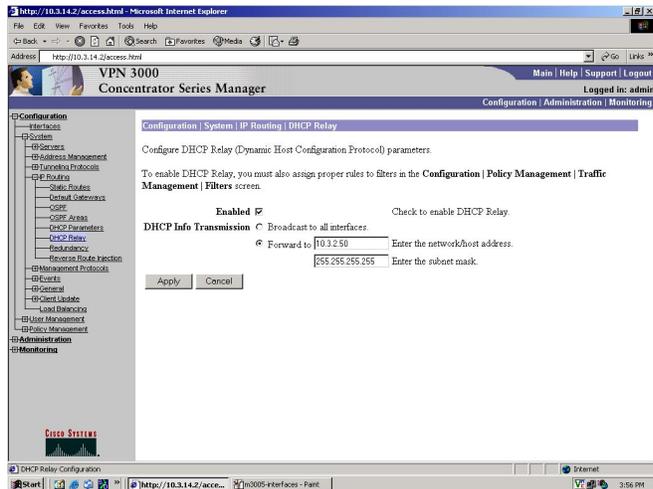
Small and Remote Office Configurations

Configurations for the small and remote designs are not provided because there are no unique configuration elements for these designs. Refer to the generic recommendations provided at the beginning of this section for guidance.

Appendix B: Wireless Security Primer

The Need for Wireless

Standard 802.11-based wireless LANs (WLANs) provide mobility to network users while maintaining the requisite connectivity to corporate resources. As laptops become more pervasive in the workplace, users are more prone to use laptops as their primary computing device, allowing greater portability in meetings and conferences and during business travel. WLANs offer organizations greater productivity per employee by providing constant connectivity to traditional networks in venues where previously unavailable.

Wireless network connectivity is not limited to enterprise use. WLANs offer increased productivity not only before and after meetings, but also outside the traditional office environment. Numerous wireless Internet service providers (WISPs) are appearing in airports, coffee shops, hotels, and conference and convention centers, enabling enterprise users to connect in public access venues.

Types of Wireless Technology

Wireless local-area networking has existed for many years, providing connectivity to wired infrastructures where mobility was a requirement to specific working environments. These early networks were based on both frequency-hopping and direct-sequencing radio technologies (described later). These early wireless networks were nonstandard implementations, with speeds ranging between 1 and 2 MB. Without any standards driving WLAN technologies, the early implementations of WLAN were relegated to vendor-specific implementation, with no provision for interoperability, inhibiting the growth of standards-based WLAN technologies. Today, several standards exist for WLAN applications: 802.11, HiperLAN, HomeRF SWAP, and Bluetooth.

Functional View

From a functional viewpoint, WLANs can be categorized as follows: peer-to-peer wireless LANs, multiple-cell wireless LANs, and building-to-building wireless networks (point to point and point to multipoint). In a peer-to-peer wireless LAN, wireless clients equipped with wireless network interface cards (NICs) communicate with each other without the use of an access point. Coverage area is limited in a peer-to-peer LAN, and wireless clients do not have access to wired resources. A multiple-cell wireless LAN extends the coverage through the use of overlapping cells. Coverage area of a cell is determined by the characteristics of the access point (a wireless bridge) that coordinates the wireless clients' use of wired resources.

Building-to-building wireless networks address the connectivity requirement between LANs (buildings) in a campus-area network. There are two different types of building-to-building wireless networks: point to point and point to multipoint. Point-to-point wireless links between buildings are radio- or laser-based point-to-point links. A radio-based point-to-point bridged link between buildings uses directional antennas to focus the signal power in a narrow beam, maximizing the transmission distance. A laser-based point-to-point bridged link between buildings uses laser light (usually infrared light) as a carrier for data transmission. A radio-based point-to-multipoint bridged network uses antennas with wide beam width to connect multiple buildings (LANs) in a campus-area network.

Technology View

Though most of this paper focuses on 802.11 WLANs (described below), it is relevant to understand other wireless standards currently in the market.

HiperLAN

HiperLAN is a European Telecommunications Standards Institute (ETSI) standard ratified in 1996. HiperLAN/1 standard operates in the 5-GHz radio band up to 24 Mbps. The ETSI has recently approved HiperLAN/2, which operates in the 5-GHz band at up to 54 Mbps using a connection-oriented protocol for sharing access among end-user devices.

HomeRF SWAP

In 1988, The HomeRF SWAP Group published the Shared Wireless Access Protocol (SWAP) standard for wireless digital communication between PCs and consumer electronic devices within the home. SWAP supports voice and data over a common wireless interface at 1 and 2-Mbps data rates using frequency-hopping and spread-spectrum techniques in the 2.4-GHz band.

Bluetooth

Bluetooth is a personal-area network (PAN) specified by the Bluetooth Special Interest Group for providing low-power and short-range wireless connectivity using frequency-hopping spread spectrum in the 2.4-GHz frequency environment.

802.11 Wireless Technology

The IEEE maintains the 802.11-based standard, as well as other 802-based networking standards, such as 802.3 Ethernet. A nonprofit, vendor-neutral organization known as the Wi-Fi Alliance provides a branding for 802.11-based technology known as Wi-Fi. A Wi-Fi compliant device must pass interoperability testing in the Wi-Fi laboratory. All vendor products that are Wi-Fi certified are guaranteed to work with all other Wi-Fi certified products—regardless of the vendor.

Standard 802.11-based wireless technologies take advantage of the radio spectrum deemed usable by the public. This spectrum is known as the Industrial, Scientific, and Medical (ISM) band. The 802.11 standard specifically takes advantage of two of the three frequency bands, the 2.4 GHz-to-2.4835 GHz UHF band used for 802.11 and 802.11b networks, and the 5.15 GHz-to-5.825 GHz SHF band used for 802.11a-based networks.

The spectrum is classed as unlicensed, meaning there is no one owner of the spectrum, and anyone can use it as long as that user's device complies with FCC regulations. Some of the areas the FCC governs include the maximum transmit power of the radios and the type of encoding and frequency modulations that can be used.

Wireless LAN Radio Frequency Methods

The 2.4-GHz ISM band (used by 802.11b) makes use of spread-spectrum technology. Spread spectrum dictates that data transmissions are spread across numerous frequencies. The reason for this is that the 2.4-GHz band has other primary owners. Primary owners are entities who have bought the spectrum for their own use, or have been granted legal access to the spectrum above all else. Common primary owners of the 2.4-GHz band include microwave oven manufacturers. Microwave ovens transmit in the same frequency range, but at far greater power levels (a typical

802.11 network card operates at 100 mW, whereas a microwave oven operates at 600W). With spread-spectrum technology, if there is ever any overlap with the primary owner, the primary owner has what can effectively be called "radio frequency (RF) right of way."

The 802.11 standard specifies two different types of Layer 1 physical interfaces for radio-based devices. One uses a frequency-hopping architecture, whereas the other uses a more straightforward single-frequency approach, known as direct sequencing.

Frequency Hopping

The 2.4-GHz ISM band provides for 83.5 MHz of available frequency spectrum. The frequency-hopping architecture makes use of the available frequency range by creating hopping patterns to transmit on one of 79 1-MHz-wide frequencies for no more than 0.4 seconds at a time (refer to Figure B-1). This setup allows for an interference-tolerant network. If any one channel stumbles across an interference, it would be for only a small time slice because the frequency-hopping radio quickly hops through the band and retransmits data on another frequency.

The major drawback to frequency hopping is that the maximum data rate achievable is 2 Mbps. Although you can place frequency-hopping access points on 79 different hop sets, mitigating the possibility for interference and allowing greater aggregated throughput, scalability of frequency-hopping technologies becomes a deployment issue. Work is being done on wide-band frequency hopping, but this concept is not currently standardized with the IEEE. Wide-band frequency hopping promises data rates as high as 10 Mbps.

Figure B-1
Frequency Hopping
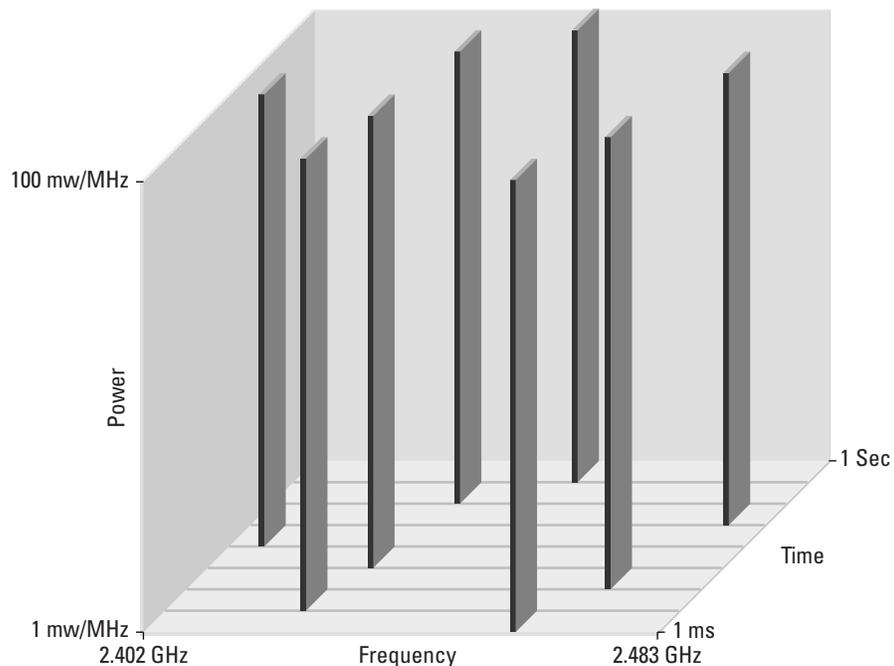
Direct Sequencing and 802.11b

Direct-sequencing networks take a different approach to data transmission. Direct sequencing provides 11 overlapping channels of 83 MHz within the 2.4-GHz spectrum. Within the 11 overlapping channels, there are 3 22-MHz-wide nonoverlapping channels (refer to Figure B-2). The large bandwidth along with advanced modulation based on complementary code keying (CCK) provided by direct sequencing is the primary reason why direct sequencing can support higher data rates than frequency hopping. Additionally, because the three channels do not overlap, three access points can be used simultaneously to provide an aggregate data rate of the combination of the three available channels. In 1999, the IEEE ratified the 802.11b standard, which provided newer, enhanced modulation types to allow direct-sequencing networks to achieve data rates as high as 11 Mbps, or 33 Mbps when the three nonoverlapping channels are used together. Direct sequencing does have one disadvantage compared to frequency hopping: interference intolerance. Though both are affected by interference, throughput in a direct-sequencing network falls dramatically when interference is introduced.

Figure B-2
Direct Sequencing
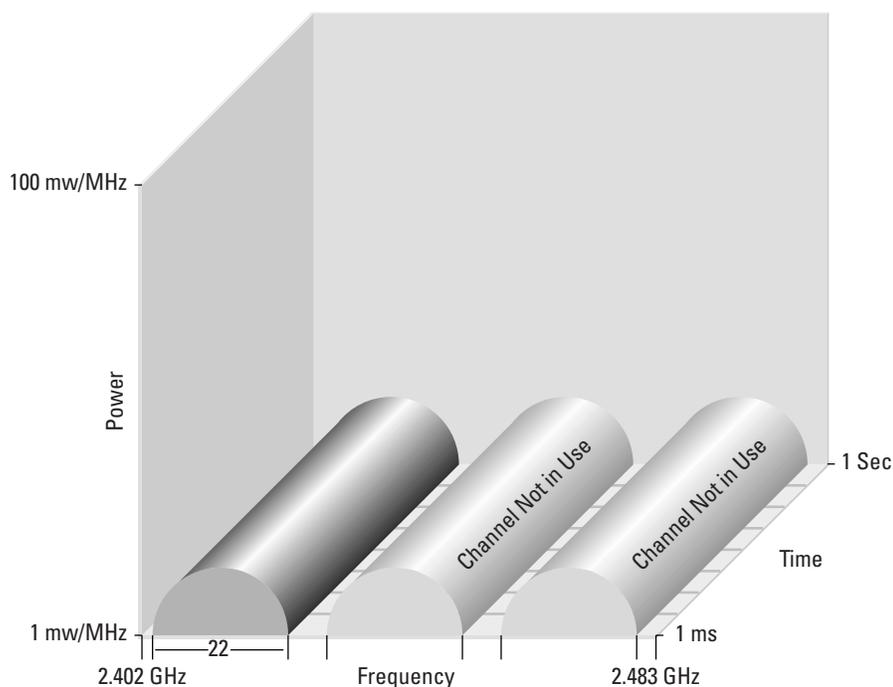
802.11a Networks

In 1999, the IEEE also ratified another Layer 1 physical interface, known as 802.11a. The 802.11a standard uses the 5-GHz SHF band to achieve data rates as high as 54 Mbps.

Unlike the 802.11 and 802.11b standards, the 802.11a standard uses a type of frequency-division multiplexing (FDM) called orthogonal FDM (OFDM). In a FDM system, the available bandwidth is divided into multiple data carriers. The data to be transmitted is then divided among these subcarriers. Because each carrier is treated independent of the others, a frequency guard band must be placed around it. This guard band lowers the bandwidth

efficiency. In OFDM, multiple carriers (or tones) are used to divide the data across the available spectrum, similar to FDM. However, in an OFDM system, each tone is considered to be orthogonal (independent or unrelated) to the adjacent tones and, therefore, does not require a guard band. Thus, OFDM provides high spectral efficiency compared with FDM, along with resiliency to radio frequency interference and lower multipath distortion.

The FCC has broken the 5-GHz spectrum into three parts, as part of the Unlicensed National Information Infrastructure (U-NII). Each of the three U-NII bands has 100 MHz of bandwidth and consists of four nonoverlapping channels that are 20 MHz wide. As a result, each of the 20-MHz channels comprises 52 300 kHz-wide subchannels. Forty-eight of these subchannels are used for data transmission, while the remaining four are used for error correction. Three U-NII bands are available for use:

- U-NII 1 devices operate in the 5.15- to 5.25-GHz frequency range. U-NII 1 devices have a maximum transmit power of 50 mW, a maximum antenna gain of 6 dBi, and the antenna and radio are required to be one complete unit (no removable antennas). U-NII 1 devices can be used only indoors.

- U-NII 2 devices operate in the 5.25- to 5.35-GHz frequency range. U-NII 2 devices have a maximum transmit power of 250 mW and maximum antenna gain of 6 dBi. Unlike U-NII 1 devices, U-NII 2 devices may operate indoors or outdoors, and can have removable antennas. The FCC allows a single device to cover both U-NII 1 and U-NII 2 spectra, but mandates that if used in this manner, the device must comply with U-NII 1 regulations.

- U-NII 3 devices operate in the 5.725- to 5.825-GHz frequency range. These devices have a maximum transmit power of 1W and allow for removable antennas. Unlike U-NII 1 and U-NII 2 devices, U-NII 3 devices can operate only in outdoor environments. As such, the FCC allows up to a 23-dBi gain antenna for point-to-point installations, and a 6-dBi gain antenna for point-to-multipoint installations.

Wireless LAN Roaming

The 802.11 specification does not stipulate any particular mechanism for roaming. Therefore, it is up to each vendor to define an algorithm for its WLAN clients to make roaming decisions.

To provide some perspective on 802.11 station roaming, we first review 802.3 Ethernet network architecture. Standard 802.3-based Ethernet LANs use the carrier sense multiple access collision detect (CSMA/CD) architecture. A station that wishes to transmit data to another station first checks to see if the medium is in use—the carrier sense function of CSMA/CD. All stations that are connected to the medium have equal access to it—the multiple access portion of CSMA/CD. If a station verifies that the medium is available for use, it begins transmitting. If two stations sense that the medium is available and begin transmitting at the same time, their frames will "collide" and render the data transmitted on the medium useless. The sending stations are able to detect a collision, the collision detection function of CSMA/CD, and run through a fallback algorithm to retransmit the frames.

The 802.3 Ethernet architecture was designed for wired networks. The designers placed a certain amount of reliability on the wired medium to carry the frames from a sender station to the desired destination. For that reason, 802.3 has no mechanism to determine if a frame has reached the destination station. The 802.3 standard relies on upper-layer protocols to deal with frame retransmission.

Standard 802.11 networks transmit across the air, and are subject to numerous sources of interference. The designers of 802.11 understood this issue, and provided a link layer acknowledgment function to provide notifications to the sender that the destination has received the frame. For every frame transmitted, the receiving station responds with an acknowledgment (ACK) frame.

Client stations use the ACK messages as a means of determining how far from the access point they have moved. As the station transmits data, it has a time window in which it expects to receive an ACK message from the destination. When these ACK messages start to time out, the client knows that it is moving far enough away from the access point that communications are starting to deteriorate.

Access points also send out periodic management frames known as beacons. Beacons contain access point information such as the service set identifier (SSID), support data rates, whether the access point supports frequency hopping or direct sequencing, and capacity. Beacon frames are broadcast from the access point at regular intervals, adjustable by the administrator.

ACK frames and beacons provide the client station with a reference point to determine whether a roaming decision needs to be made. If a set number of beacon messages are missed, the client can assume they have roamed out of range of the access point with which they are associated. In addition, if expected ACK messages are not received, clients can also make the same assumption.

The actual act of roaming can differ from vendor to vendor. The basic act of roaming is making a decision to roam, followed by the act of locating a new access point to roam to. This scenario can involve reinitiating a search for an access point, in the same manner the client would when it is initialized, or other means, such as referencing a table built during the previous association.

The timing of WLAN roams also varies according to vendor, but in most cases is less than 1 second, and in the best cases, less than 200 msec. It is also important to note that because roaming is vendor specific, roaming between different vendors' access points can have extended roam times.

Wireless Security

As standardized by the IEEE, security for 802.11 networks can be simplified into two main components: encryption and authentication. The implementation of these components has been proven and documented as insecure by the security community at large. They are presented here so the reader can understand the fundamental flaws when they are presented in the axioms section of this document.

Frame Encryption

Properly performed encryption allows for confidentiality. Encryption is the process of taking a message, referred to as cleartext, and passing it through a mathematical algorithm to produce what is known as ciphertext. Decryption is the reverse of the process. Encryption algorithms typically rely on a value, called a key, in order to encrypt and decrypt the data. Two major forms of encryption are used today—symmetric encryption (also known as shared-key encryption) and asymmetric encryption (also know as public or private encryption). Symmetric encryption is about 1000 times faster than asymmetric encryption, and is, therefore, used for the bulk encryption of data. Generally with well-designed encryption algorithms, longer keys result in a higher degree of security because more brute force is required to try every possible key (known as the key space) in order to decrypt a message. The IEEE has specified that wired equivalent privacy (WEP) be the means to encrypt 802.11 data frames. WEP uses the RC4 stream cipher that was invented by Ron Rivest of RSA Data Security, Inc. (RSADSI) for encryption. The RC4 encryption algorithm is a symmetric stream cipher that supports a variable-length key. A stream cipher is one that operates the encrypt or decrypt function on a unit of plaintext (in this case, the 802.11b frame). This cipher is contrasted with a block cipher, which processes a fixed number of bytes in each encrypt or decrypt function. With symmetric encryption, the key is the one piece of information that must be shared by both the encrypting and decrypting endpoints. RC4 allows the

key length to be variable, up to 256 bytes, as opposed to requiring the key to be fixed at a certain length. IEEE specifies that 802.11 devices must support 40-bit keys, with the option to use longer key lengths. Several vendors support 128-bit WEP encryption with their WLAN solutions.

Because WEP is a stream cipher, a mechanism is required to ensure that the same plaintext will not generate the same ciphertext. The IEEE stipulated the use of an initialization vector to be concatenated with the symmetric key before generating the stream ciphertext.

The initialization vector is a 24-bit value (ranging from 0 to 16777215). The IEEE suggests—but does not mandate—that the initialization vector change per frame. Because the sender generates the initialization vector with no standard scheme or schedule, it must be sent to the receiver unencrypted in the header portion of the 802.11 data frame. The receiver can then concatenate the received initialization vector with the WEP key (base key) it has stored locally to decrypt the data frame. As illustrated in Figure B-3, the plaintext itself is not run through the RC4 cipher, but rather the RC4 cipher is used to generate a unique keystream for that particular 802.11 frame using the initialization vector and base key as keying material. The resulting unique keystream is then combined with the plaintext and run through a mathematical function called XOR. This produces the ciphertext.

Figure B-3
WEP Encryption Process
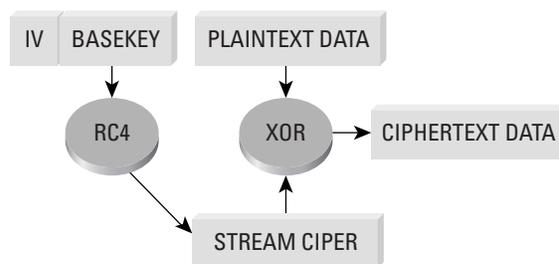
Authentication Mechanism

The IEEE specified two authentication algorithms for 802.11-based networks. First, open authentication is a null authentication algorithm because any station requesting authentication is granted access. The second form of authentication is called shared-key authentication, which requires that both the requesting and granting stations be configured with matching WEP keys. The requesting stations send an authentication request to the granting station. The granting station sends a plaintext challenge frame to the requesting station. The requesting station WEP encrypts the challenge frame and sends it back to the granting station. The granting station attempts to decrypt the frame, and if the resulting plaintext matches what the granting station originally sent, then the requesting station has a valid key and is granted access.

Note that shared-key authentication has a known flaw in its concept. Because the challenge packet is sent in the clear to the requesting station and the requesting station replies with the encrypted challenge packet, an attacker can derive the stream cipher by analyzing both the plaintext and the ciphertext. This information can be used to build decryption dictionaries for that particular WEP key. The known insecurities with WEP as standardized in the IEEE are discussed in the axioms section of this document.

Wireless LAN Components

Components of a WLAN are access points, NICs or client adapters, bridges, and antennas.

- *Access point*—An access point operates within a specific frequency spectrum and uses a 802.11 standard specified modulation technique. It also informs the wireless clients of its availability and authenticates and associates wireless clients to the wireless network. An access point also coordinates the wireless clients' use of wired resources.

- *NIC or client adapter*—A PC or workstation uses a wireless NIC to connect to the wireless network. The NIC scans the available frequency spectrum for connectivity and associates it to an access point or another wireless client. The NIC is coupled to the PC or workstation OS using a software driver.

- *Bridge*—Wireless bridges are used to connect multiple LANs (both wired and wireless) at the Media Access Control (MAC) layer level. Used in building-to-building wireless connections, wireless bridges can cover longer distances than access points (IEEE 802.11 standard specifies 1 mile as the maximum coverage range for an access point).

- *Antenna*—An antenna radiates the modulated signal through the air so that wireless clients can receive it. Characteristics of an antenna are defined by propagation pattern (directional versus omnidirectional), gain, transmit power, and so on. Antennas are needed on both the access point and bridge and the clients.

Appendix C—Rogue Access Point Additional Information

As discussed in the document, the threat posed by rogue access points can be mitigated. This appendix provides detailed guidance on minimizing the risk that rogue access points represent to enterprise networks using the following:

Prevention
- Corporate policy
- Physical security
- Supported WLAN infrastructure
- Standard 802.1X port-based security on edge switches

Detection
- Using wireless analyzers or sniffers
- Using scripted tools on the wired infrastructure
- Physically observing WLAN access point placement and usage

At the end of the appendix is a listing of wireless sniffers and known Media Access Control (MAC) addresses. This information can assist in the detection and prevention of rogue access points.

Preventing Rogue Access Points

The first priority for enterprise IT security departments should be to prevent rogue access points in the first place. Rogue access point prevention can be achieved with a combination of the following:

- Create and publish a policy banning employee installations of wireless LAN (WLAN) equipment.
- Provide for physical security.
- Provide a supported WLAN infrastructure—removing the motivation for employee installs.

- Implement IEEE 802.1X port-based security.
- Use Layer 2 and 3 switch filters.

Create a Corporate WLAN Policy

An enterprise policy concerning WLAN installations is an essential first step in preventing rogue access points. The WLAN policy should include who is authorized to install WLAN access points, and what security policies must be complied with when they are installed. For instance, the policy should dictate which security scheme the access point must utilize for secure client connectivity.

Physical Security

Physical security also plays a part in rogue access point prevention. Physical security standards should be in place to prevent an intruder from gaining unauthorized access to the enterprise premises or to detect the intruder if physical access is gained.

Provide a Supported WLAN Infrastructure

Given that almost all rogue access points are installed by a nonmalicious (frustrated insider) class of users, the best way to prevent such rogue installs is to remove the motivation for them. Installing a managed, supported, and secure WLAN network throughout the enterprise removes the motivation for employees to install rogue access points. Frustrated insiders are categorized as those who install an unauthorized access point in order to provide wireless coverage where none is officially available; for example, enabling wireless networking in a meeting room, cafeteria, outdoor space, or other common area. The wide availability of low-cost access points has made this installation type very easy. The threat posed by this class of install is that the person installing the access point is often ignorant of security features that are necessary to prevent outsiders from accessing the enterprise network, and the consumer grade access point commonly used in this installation does not have the features to provide an enterprise level of security.

Using IEEE 802.1X

Recent access layer switches support an IEEE standard called 802.1X, which provides port-based security. With 802.1X enabled on switches and access points at the edge of the network, no device can be connected unless the device is able to 802.1X authenticate to a Remote Access Dial-In User Service (RADIUS) server behind the switch. It is recommended that 802.1X be disabled only on all authorized access point switch ports. This in turn pushes 802.1X user authentication to the wired and wireless edge of the enterprise. Further discussion of 802.1X technology is included later in the document in the section "Security Extensions Are Required."

Using Layer 2 or 3 Switch Filters

This section looks at ways in which Layer 2 and 3 switch features might be used to prevent rogue access points. Table C-1 lists the methods that are investigated.

Table C-1 Methods Investigated

Method	Summary of Method
Using Cisco Catalyst® switch filters to limit MAC addresses per port	Limiting the number of MAC addresses that can be used per port can prevent switches from passing traffic from rogue access point clients.
Using Cisco Catalyst switch filters to drop frames from third-party access points	The possibility of configuring the switch to drop frames from vendors of third-party access points and third-party wireless network interface cards (NICs) was investigated. This option is not feasible because switches do not support wild-card masks on MAC address filters.

Limitations of Using Filters to Prevent Rogue Access Points from Connecting to the Enterprise Network

- Filters designed to prevent a vendor's access points will also prevent that vendor's NICs. For example, preventing vendor A access points could also prevent vendor A Ethernet NICs.

- Traffic coming through an access point has the MAC address of the wireless NIC, not of the access point. For example, if an access point from vendor A is connected to a port with a vendor A MAC filter on it, it would still be able to pass traffic from a vendor B or vendor C wireless NIC. The resolution for this issue would be to use a command (if wildmask MACs were configurable) to shut down the port if an unauthorized MAC was seen.

- WLAN access point vendors will come and go, and there will never be an authoritative list of all access point vendors' MAC Organizational Unique Identifiers (OUIs).

- MAC addresses can be changed or spoofed.

Detecting Rogue Access Points

In addition to the rogue access point prevention mechanisms mentioned in the previous section, a combination of the following rogue access point detection methods should also be used by the IT security administrator:

- Detecting rogue access points wirelessly
- Detecting rogue access points from the wired network
- Detecting rogue access points by physical observation

Detecting Rogue Access Points Wirelessly

Detecting rogue access points wirelessly is the process of using WLAN hardware and software to detect rogue access points.

Table C-2 lists the advantages and disadvantages of wireless detection of rogue access points.

Table C-2 Advantages and Disadvantages of Wireless Detection of Rogue Access Points

Wireless Detection Advantages	Wireless Detection Caveats
• Often picks up access points that the other rogue access point detection methods miss • Is very effective at detecting access points installed by the nonmalicious (*frustrated insider*) class of installer (default security options or broadcast service set identifier [SSID])	• This method requires that the WLAN device be within range of an access point to be able to detect it and may require that the IT security administrator perform a walkthrough of the enterprise campus with a wireless analyzer. • Many tools do not see access points that do not broadcast their SSID. • IT security administrator cannot easily survey remote sites. • WLAN access point signals may be difficult to pick up because of building materials that block 802.11 signals.

Many WLAN analyzers are available, and to various degrees they are capable of detecting rogue access points. See section "Wireless Analyzers" in this appendix for a listing of some of the wireless analyzers that can be used for detecting rogue access points. When a WLAN analyzer detects a suspected rogue access point, a direction antenna on the analyzer is a very useful aid in locating the access point.

Detecting Rogue Access Points from the Wired Network

Rogue access points can be detected from the wired network using:

- MAC addresses
- OS fingerprinting
- Simple Network Management Protocol (SNMP)
- Intrusion detection

A large number of software tools are available to aid in detecting rogue access points from a wired management station on the Ethernet portion of the network.

Table C-3 lists the advantages and disadvantages of wired detection of rogue access points.

Table C-3 Advantages and Disadvantages of Wired Detection of Rogue Access Points

Advantages	Disadvantages
• It is easier to monitor networks on a more "real-time" basis. • It uses automated scripts, which require less manpower to operate. • This method makes it possible to survey remote sites.	• This method can miss some rogue access points. • Most of the software is immature or not specifically written to detect rogue access points. • This method may create a lot of false positives on intrusion detection systems and personal firewalls.

Using MAC Addresses

MAC address monitoring tools rely on detecting rogue access points by looking for a known MAC address, or by cataloging all authorized MAC addresses in the network and looking for new ones. The latter approach has the advantage of alerting when an unauthorized non-access point device, such as an unauthorized laptop, is connected to the network. This approach also has more of a problem with false positives. Known MAC address monitoring tools are listed in Table C-4.

Table C-4 Known MAC Address Monitoring Tools

Access Point tools	• http://aptools.sourceforge.net/wireless.ppt
	• http://aptools.sourceforge.net/
	Access point tools can discover an access point based on MAC address, and then check that it is an access point (not a wireless NIC) via Hypertext Transfer Protocol (HTTP); these tools can also check security settings (wired equivalent privacy [WEP]) and SNMP settings via HTML.
Arpwatch	• http://www-nrg.ee.lbl.gov/
	Arpwatch monitors Ethernet activity and keeps a database of Ethernet or IP address pairings; it also reports certain changes via e-mail.

Using Operating System Fingerprinting

These tools can be utilized to fingerprint an OS, such as the OS on an access point. OS fingerprinting works by observing particular characteristics of individual OSs such as the way they respond to TCP packets with obscure TCP flags and options enabled. OS fingerprinting tools are capable of correctly identifying some access points, but the extent of matching the OS to rogue access points is dependent on the tool having a fingerprint match for the access point vendor OS. Table C-5 lists the known fingerprinting tools.

Table C-5 Known OS Fingerprinting Tools

NMAP	• http://www.insecure.org/nmap/index.html
	• http://www.insecure.org/nmap/nmap-fingerprinting-article.html
	A very well-known, popular, and respected tool; NMAP is unproven as a rogue access point detection tool, but it may be useful in conjunction with other rogue access point detection techniques. It generates a lot of alerts in intrusion detection and personal firewall systems.
Xprobe	• http://www.sys-security.com/html/projects/X.html
	Xprobe 1 combines various remote active OS fingerprinting methods using the Internet Control Message Protocol (ICMP), which was discovered during the "ICMP Usage in Scanning" research project, into a simple, fast, efficient, and powerful way to detect an underlying OS that a targeted host is using.
	Xprobe 2 is an active OS fingerprinting tool with a different approach to OS fingerprinting; it relies on fuzzy signature matching, probabilistic guesses, multiple matches simultaneously, and a signature database.
	Xprobe is unproven as a rogue access point detection tool, but it may be useful in conjunction with other rogue access point detection techniques. It generates a lot of alerts in intrusion detection and personal firewall systems.

Using SNMP

SNMP is not thought to be a very effective way to detect rogue access points. Most rogue access points probably would not have SNMP enabled, and even if they did, SNMP community strings would probably be unknown. If an SNMP tool is required for rogue access point detection, existing enterprise management packages have the capability to do IP and SNMP discovery.

Detecting Rogue Access Points Physically

IT security administrators can also detect unauthorized WLAN activity by physically observing the work environment. IT security administrators should be alert for the following:

- Unauthorized WLAN access points in visible locations
- Employees using WLAN access in a location where WLAN access should not be available
- Warchalk symbols denoting WLAN availability (see http://www.warchalking.org/ for more information)

In summary, individually each current rogue access point prevention or detection method is limited. It is recommended that network designers choose a combination of prevention and detection tools for their network. As discussed, each prevention or detection tool presents a different capability and can be used in combination with another tool in order to provide the network designer a comprehensive acceptable rogue access point prevention and detection toolset.

Wireless Analyzers

Table C-6 below lists commonly used wireless analyzers.

Table C-6   List of Wireless Analyzers

Airmagnet	• www.airmagnet.com A commercial product, Airmagnet is a full-featured WLAN site-survey tool that runs on a Compaq iPaq.
Boingo	• www.boingo.com Boingo is free software that can be downloaded from the Internet; it searches all available networks, and lets you know when you are in the range of a high-speed service signal (or tells you where to find the closest one).
Netstumbler	• http://www.netstumbler.org/ Very popular and well known, Netstumbler is free software that can be downloaded from the Internet; it detects WLAN access points and displays information about them.
Sniffer	• www.sniffer.com This professional wireless analyzer could possibly be used to help look for rogue APaccess points by defining filters to look for beacons, but to exclude authorized SSIDs, or by defining filters to look for the MAC OUIs of known APaccess point vendors.
Wildpackets	• http://www.wildpackets.com/products/airopeek This professional wireless analyzer could possibly be used to help look for rogue access points by defining filters to look for beacons, but to exclude authorized SSIDs, or by defining filters to look for the MAC OUIs of known access point vendors.

Table C-6   List of Wireless Analyzers

Observer	• http://www.networkinstruments.com/ This tool could possibly be used to help look for rogue access points by defining filters to look for beacons, but to exclude authorized SSIDs, or by defining filters to look for the MAC OUIs of known access point vendors.
Finisar Surveyor	• http://www.gofinisar.com/products/protocol/wireless/surveyor_w.html This tool could possibly be used to help look for rogue access points by defining filters to look for beacons, but to exclude authorized SSIDs, or by defining filters to look for the MAC OUIs of known access point vendors.
Wellenreiter	• http://www.remote-exploit.org/ Similar to Netstumbler but less popular and not as well known, Wellenreiter detects WLAN access points and displays information about them.
Kizmet	• http://www.kismetwireless.net/ Kismet is an open source wireless sniffer that could possibly be used to help look for rogue access points by defining filters to look for beacons, but to exclude authorized SSIDs.
dachb0den	• http://www.dachb0den.com/projects/bsd-airtools.html This tool, which is not well known, seems to be a combination of Netstumbler and Airsnort functionality.
Hornet	• http://www.bvsystems.com/Products/WLAN/Hornet/hornet.htm This dedicated hardware looks for a list of access point MAC addresses that have been configured and downloaded from a PC. It does not seem to do anything that a WLAN sniffer cannot do.
IBM Distributed Wireless Security Auditor	• http://www.research.ibm.com/gsal/dwsa/ This tool is a prototype only; it is not for sale. It uses client software on enterprise NICs to detect and report on all detected access points and their security system; a back-end system compares the list of detected access points with a list of authorized access points and alerts on unknown access points. This tool might produce false positives.
IBM TP General—IBM Access Connections for Windows 2000/XP	• http://www.pc.ibm.com/qtechinfo/MIGR-4ZLNJB.html Access Connections is a connectivity assistant program for your ThinkPad computer. It enables you to quickly switch the network settings and Internet settings by selecting a location profile. You can define the network settings and Internet settings in the Location Profile for modem or /wired LAN or /wireless LAN network devices, and then restore that profile whenever you need it. By switching the location profile, you can connect to the network instantly without reconfiguring your settings when you move from office to home or go on the road.

Known Access Point MAC Addresses

Table C-7 provides a partial list of MAC OUIs used by access point vendors. This table was obtained from the *aptools* site at aptools.sourceforge.net.

Table C-7 MAC OUIs Used by Access Point Vendors

Manufacturer	MAC Address Range
3Com	0001.03|0004.76|0050.da|0800.02
Addtron	0040.33|0090.d1
Advanced Multimedia Internet	0050.18
Apple	0030.65
Atmel	0004.25
Bay Networks	0020.d8
BreezeNet	0010.e7
Cabletron (Enterasys)	0001.f4|00e0.63
Camtec	0000.ff
Cisco Aironet	0040.96
Compaq	0050.8b
D-Link	0005.5d|0040.05|0090.4b
Delta Networks	0030.ab
Intel	0002.b3
Linksys	0003.2f|0004.5a
Lucent	0002.2d|0060.1d|0202.2d
Nokia	00e0.03
Samsung	0000.f0|0002.78
Senao Intl	0002.6f
SMC	00e0.29|0090.d1
SOHOware	0080.c6
Sony	0800.46
Symbol	00a0.f8|00a0.0f
Z-Com	0060.b3
Zoom	0040.36

Appendix D—Network Availability

The following sections describe in detail items that should be considered when deploying services in order to secure wireless LANs (WLANs). Note that in the remote, small, and medium network designs, high availability is not provided in the Cisco SAFE Blueprint for network security wired network, so it is not expected to be present for wireless.

Dynamic Host Configuration Protocol

- *Requests per second*—The Dynamic Host Configuration Protocol (DHCP) server hardware and software must be able to accommodate the projected number of new DHCP requests per second that will be offered by introducing WLANs. If the DHCP servers are overburdened, wireless users will not be able to acquire DHCP addresses, denying Extensible Authentication Protocol (EAP) users from gaining IP connectivity after authentication and denying IP security (IPsec) users from setting up a secure tunnel with the virtual-private-network (VPN) gateways.

- *DHCP Safe Failover Protocol*—Network designers should implement DHCP servers that provide redundancy on dual servers via the draft RFC DHCP Safe Failover Protocol. By implementing this protocol, network designers can increase network availability for their wireless end users.

- *Address management*—Network designers should consider the additional IP addressing requirements that are introduced by implementing WLANs. Also, if the network designer chooses to use IPsec VPNs to secure the wireless environment, additional IP addressing is required for the VPN tunnels that are built. If DHCP services are not available in either case, wireless users will be denied access to the corporate network.

- *Network design considerations*—Network designers must consider where the DHCP services are located in relation to the end users accessing the services. A redundant network is required between the two locations in order to achieve high availability. Also, it is recommended that network designers not group all their DHCP services in one subnet because a denial-of-service (DoS) attack against the subnet can deny DHCP service to all wireless users.

RADIUS

- *Requests per second*—The Remote Access Dial-In User Service (RADIUS) server hardware and software must be able to accommodate the projected number of new RADIUS requests per second that will be offered by introducing WLANs. If the RADUIS servers are overburdened, wireless access point and VPN gateways will not be able to authenticate users, denying wireless users connectivity to the corporate network. Also, it should be noted that if the network designer elects to use a back-end database for user authentication, the back-end database must also be designed to accommodate the projected number of user authentication requests per second that will be offered by introducing WLANs.

- *Redundant server deployment*—Multiple RADIUS servers should be deployed in order to give the authenticating device (wireless access point or VPN gateway) redundant options for servicing authentication requests. Network designers should also group the authenticating devices to alternate the listing of primary and secondary RADIUS servers. This setup accomplishes two goals: it limits the failure domain in the case of a server failure and also enables each RADIUS server to scale more effectively.

- *User management*—RADIUS servers need to provide high-availability access to the user database required for user authentication. Network designers should consider implementing servers that synchronize data if the user database is to be stored locally. This setup allows a single point of administration and eliminates the possibility

of a user definition being on one RADIUS server but not the other. If the user database is stored externally (Lightweight Directory Access Protocol [LDAP], NT domain), network designers should consider the location of the RADIUS servers to the back-end database because a network outage between the two resources can deny wireless users access to the corporate network.

IP Security Protocol

- *Connections per second*—The VPN gateway hardware and software must be able to accommodate the projected number of new IPsec connections per second that will be offered by introducing WLANs.

- *Encryption throughput*—The VPN gateway hardware and software must be able to accommodate the projected encryption throughput that will be offered by introducing WLANs. VPN gateways work harder to encrypt several smaller packets than one larger packet, causing lower encryption throughput numbers for the VPN gateway. It is important that network designers understand the packet size distribution of their wired networks in order to properly size the VPN gateway for the wireless network environment.

- *Simultaneous IPsec sessions*—The VPN gateway hardware and software must be able to accommodate the projected number of simultaneous IPsec sessions that will be offered by introducing WLANs. VPN gateways are designed to handle a finite limit of simultaneous IPsec sessions.

Failure to design the IPsec environment with these considerations in mind will cause the wireless users to be unable to access the corporate network, or when they do so, performance will be severely degraded. VPN vendors have addressed the previous three items by introducing proprietary clustering technologies. The clustering technologies load balance new IPsec connections to the least-loaded VPN gateway in order to give the new IPsec connection the best possible service.

More in-depth information on designing IPsec networks can be found in "SAFE VPN: IPsec Virtual Private Networks in Depth."

References

Cisco SAFE White Papers

SAFE: A Security Blueprint for Enterprise Networks:

http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safe_wp.htm

SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks:

http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safes_wp.htm

SAFE VPN: IPsec Virtual Private Networks in Depth:

http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safev_wp.htm

Cisco Aironet® Wireless LAN Security white papers:

http://www.cisco.com/go/aironet/security

SAFE: Nimda Attack Mitigation:

http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/snam_wp.htm

SAFE: Code-Red Attack Mitigation:

http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/scdam_wp.htm

Miscellaneous References

Security of the WEP Algorithm:

http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html

Your 802.11 Wireless Network has No Clothes:

http://www.cs.umd.edu/~waa/wireless.pdf

Weaknesses in the Key Scheduling Algorithm of RC4:

http://www.cs.umd.edu/~waa/class-pubs/rc4_ksaproc.ps

Using the Fluhrer, Mantin, and Shamir Attack to Break Wired Equivalent Privacy (WEP):

http://www.cs.rice.edu/~astubble/wep/wep_attack.pdf

AirSnort:

http://airsnort.sourceforge.net/

Partner Product References

RSA SecureID OTP System

http://www.rsasecurity.com/products/securid/

Acknowledgments

The authors would like to publicly thank all the individuals who contributed to this extension of the SAFE blueprint and the writing of this document. Certainly, the successful completion of this document would not have been possible without the valuable input and review feedback from all of the Cisco employees both in corporate headquarters and in the field. Several individuals provided extra effort in either the review stage or lab validation. The core of this group included Greg Abelar, Andy Balinsky, Brian Cox, Roland Saville, and Ido Dubrawsky. Thank you all for your special effort.

1. Borisov et al., "Security of the WEP Algorithm"

CISCO SYSTEMS

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the Cisco Web site at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland
Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland
Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden
Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe