Cisco Systems

White Paper

SAFE: Wireless LAN Security in Depth

Authors

Sean Convery (CCIE #4232) and Darrin Miller (CCIE #6447) are the primary authors of this white paper. Mark Doering, Pej Roshan, and Sri Sundaralingam provided significant contributions to this paper and are the lead architects of Cisco's reference implementation in San Jose, CA USA. All are network architects focusing 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 SAFE blueprints. 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 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 designs

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.

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 WLAN.

Following the guidelines in this document does not guarantee a secure environment, nor does it guarantee that you will prevent all penetrations. This is particularly true with wireless networks today. As this document shows, there is no way to achieve absolute security in a wireless LAN. Realize that by deploying wireless LANs in a network you are increasing the security risk over being purely wired. This paper discusses how to mitigate those risks as much as possible, keeping in mind that it is impossible to reduce them to zero. Many organizations have decided to deploy wireless technology despite the inherent security risks that they introduce. These organizations view the productivity gains of a wireless network as outweighing any security vulnerability that is introduced into their environment. This paper addresses their concerns, as well as the concerns of the security community, which is leery of deploying WLANs in the first place.

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

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 wireless networks to wired network resources
- Wireless data confidentiality
- Access-point (AP) management
- Authentication of users to network resources
- Options for high availability (large enterprise only)

First and foremost, SAFE wireless needs to provide an alternate connectivity option to users who primarily use wired LANs. As an alternative connectivity option, it does not need to provide access to every service and host available to the wired network, but it should strive to do so as much as the organization's security policy allows. 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. This is not as easy as it seems. Finally, it must integrate with existing network designs based on the SAFE security architecture.

SAFE Wireless LAN 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 rate faster than most IT departments can keep up with. 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, this wide deployment attracted the attention of the hacker community. Several Web sites have now started documenting all the freely available wireless connections nationwide. 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 because unlike a wired network, wireless networks send data over the air and usually extend beyond the physical boundary of an organization. In particular, when strong directional antennas are used, a WLAN can reach well outside the buildings that it is designed for. This scenario creates an environment where traditional physical security controls are ineffective because the packets can be viewed by anyone within radio frequency range. For example, a person with a LINUX laptop and a program such as TCPDUMP can take advantage of this concern and receive and store all packets circulating on a given WLAN.

It is also easy to interfere with wireless communications. A simple jamming transmitter can make communications impossible. For example, consistently hammering an AP 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 can reduce the range and usable bandwidth of WLAN technology. “Bluetooth” technology, used to communicate between handsets and other information appliances, is one of many technologies today that use the same radio frequency as WLAN devices. These intentional, or unintentional, denial-of-service (DoS) attacks can render WLAN devices unusable.

General Security Vulnerabilities

Most WLAN devices use direct sequencing spread spectrum (DSSS) communications. As most WLAN devices are standards based we must assume that the attacker has a WLAN card that can be tuned onto the same spreading sequence; therefore, DSSS technology alone is neither a privacy nor an authentication feature.

The 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 AP 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 AP. The range varies, depending on the type of WLAN system. Laptop and desktop computers equipped with 802.11b 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, ship with ad hoc mode enabled by default. Any hacker who also is also configured for ad hoc mode is immediately connected to PCs using these cards and could attempt to gain unauthorized access. Although mitigating these attacks is the focus of this paper, there are some base level recommendations that every WLAN device should follow. At a minimum, the following should be done:

- Access point security recommendations:
  - Enable user authentication 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.
  - Limit management traffic to a dedicated wired subnet.
  - Encrypt all management traffic where possible.
  - Enable wireless frame encryption where available.
- Client security recommendations:
  - Disable ad hoc mode.
  - Enable wireless frame encryption where available.

Wireless Networks are Weapons

In the hands of a determined hacker, a rogue AP can be a valuable asset in the attempted compromise of network resources. The principal threat is installing an AP into a network after gaining unauthorized access to a building. The user typically gains access to the building by “tailgating” behind a user with a valid access badge or by obtaining a guest badge for some other reason. Because APs are relatively small and can be purchased at many electronics outlets worldwide, it is easy for the hacker not only to obtain the AP but also to install it discreetly. Attaching the AP to the underside of a conference-room table and plugging into the live network allows the hacker to break into a network from the relative security of his car in the parking lot. Also consider the possibility of man-in-the-middle (MITM) attacks. Using a device that can masquerade as a trusted AP, a hacker could manipulate wireless frames as they cross his device.

Policies and procedures are the two main weapons an organization has to combat this threat. From a policy perspective, Cisco recommends that an organization have a complete wireless network policy in addition to its overall security policy. This wireless policy should, at a minimum, disallow the connection of non-IT supported APs into the network. On the procedures side, the IT department needs to conduct regular scans of its office space to check for rogue APs. This includes both physical searches and wireless scans. Several vendors offer tools designed to discover the presence of the wireless APs in a certain area.

From an implementation perspective, many Ethernet switches today offer the ability to limit access to a particular port based on the MAC address of the connecting client. These controls could be set up to learn the first MAC address to connect to a port and then prevent any subsequent MAC addresses to connect. The controls could also be configured in a manner to prevent more than a fixed number of MAC addresses to connect. Both of these features can help with the rogue AP problem, but remember that their use involves a significant administrative penalty. Managing the MAC address tables in a large enterprise could become a full-time job by itself. Also remember that with a conference room it is difficult to know what different systems will connect to a given network port. Because a conference room is a likely target of a hacker with a rogue AP, it may be useful to disable wired network access from all conference rooms. After all, providing wireless access to the network from conference rooms is one of the main reasons organizations choose to deploy wireless LAN technology today.

802.11b is Insecure

As discussed in the primer section of this document, 802.11b is the most widely deployed WLAN technology today. Unfortunately, the foundation of the security of 802.11b is based on a frame encryption protocol called Wired Equivalent Privacy (WEP). This axiom discusses the problems with WEP in some detail. A good portion of the rest of this document provides solutions for this problem.

WEP (Wired Equivalent Privacy)

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 the same secret key be shared by all communicating parties. 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. As of the time this paper was written, on a busy network, 128-bit static WEP keys can be obtained in as little as 15 minutes. These attacks are described in more detail below.

As mentioned in the primer, 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 due to 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 (IV) is transmitted as plaintext and placed in the 802.11 header, anyone sniffing a WLAN can see it. At 24 bits long, the IV provides a range of 16,777,216 possible values. A University of California at Berkeley paper found that when the same IV is used with the same key on an encrypted packet (known as an IVcollision), 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 at 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 .

Recently, cryptanalysts Fluhrer, Mantin, and Shamir discovered inherent shortcomings with the RC4 key scheduling algorithm. Because RC4 as implemented in WEP chose to use a 24-bit IV 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 IVs that can be generated by RC4, and highlights methods to break the key using certain patterns in the IVs. 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/.

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" is working on standardizing WLAN 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 DHCP/DNS server. IPSec provides for confidentiality of IP traffic, as well as authentication and antireplay capabilities. Confidentiality is achieved through encryption using a variant of the Data Encryption Standard (DES), called Triple DES (3DES), which encrypts the data three times with up to three different keys.

Though IPSec is used primarily for data confidentiality, extensions to the standard allow for user authentication and authorization to occur as part of the IPSec process. This scenario offers a potential solution to the user differentiation problem with WLANs outlined later in this paper. For more information on IPSec, refer to the VPN primer in the SAFE VPN paper at the following URL: http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safev_wp.htm .

EAP/802.1X

An alternative WLAN security approach focuses on developing a framework for providing centralized authentication and dynamic key distribution. A proposal jointly submitted to the IEEE by Cisco Systems, Microsoft, and other organizations introduced an end-to-end framework using 802.1X and the Extensible Authentication Protocol (EAP) to provide this enhanced functionality. Central to this proposal are two main elements:

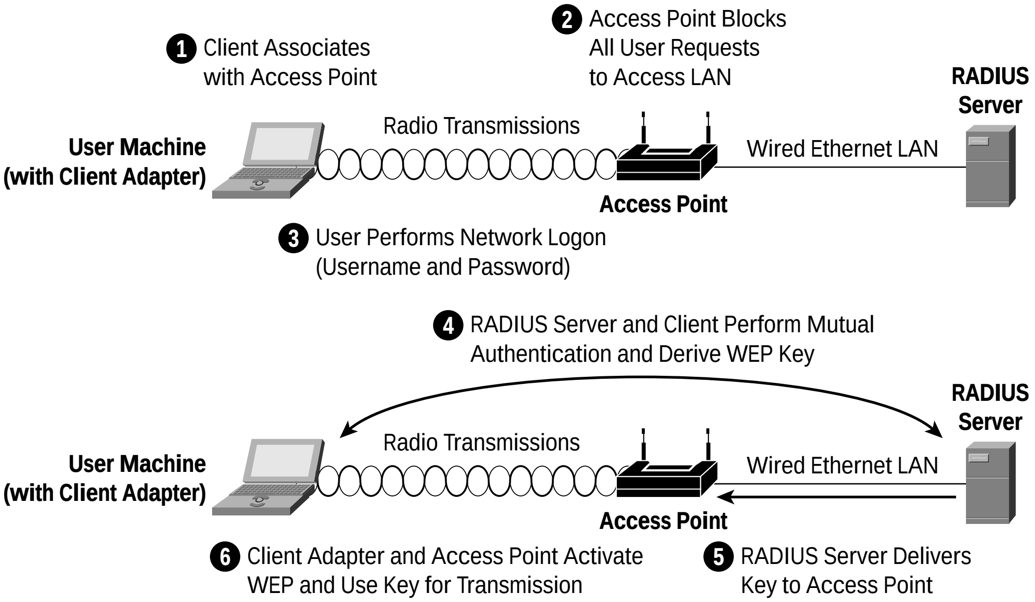
- EAP allows wireless client adapters, that may support different authentication types, to communicate with different back-end servers such as Remote Access Dial-In User Service (RADIUS)
- IEEE 802.1X, a standard for port based network access control

When these features are implemented, a wireless client that associates with an AP cannot gain access to the network until the user performs a network logon. When the user enters a username and password into a network logon dialog box or its equivalent, the client and a RADIUS server perform a mutual authentication, with the client authenticated by the supplied username and password. 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:

- 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 a username and password in a network logon dialog box or its equivalent.
- Using 802.1X and EAP, the wireless client and a RADIUS server on the wired LAN perform a mutual authentication through the access point. One of several authentication methods or types can be used. With the Cisco authentication type LEAP, 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 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.
- Both the session key and broadcast key are changed at regular intervals as configured in the RADIUS server.

Figure 1 LEAP Authentication Process


1 Client Associates with Access Point
2 Access Point Blocks All User Requests to Access LAN
RADIUS Server
Radio Transmissions
User Machine (with Client Adapter)
Wired Ethernet LAN
Access Point
3 User Performs Network Logon (Username and Password)
4 RADIUS Server and Client Perform Mutual Authentication and Derive WEP Key
RADIUS Server
Radio Transmissions
User Machine (with Client Adapter)
Wired Ethernet LAN
Access Point
6 Client Adapter and Access Point Activate WEP and Use Key for Transmission
5 RADIUS Server Delivers Key to Access Point

LEAP provides two significant benefits over basic WEP. The first benefit is the mutual authentication scheme as described above. This scheme effectively eliminates "man-in-the-middle attacks" introduced by rogue access points and RADIUS servers. The second benefit is a centralized management and distribution of the encryption keys used by WEP. Even if the

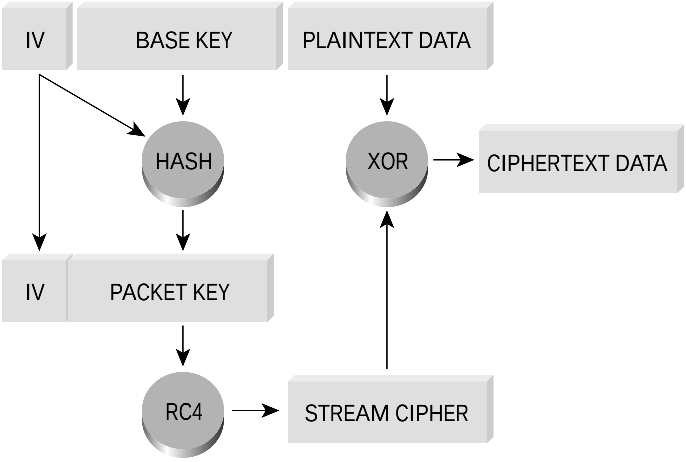
WEP implementation of RC4 had no flaws, there would still be the administrative difficulty of distributing static keys to all the APs and clients in the network. Each time a wireless device was lost, the network would need to be re-keyed to prevent the lost system from gaining unauthorized access.

WEP Improvements

WEP Key Hashing

Because the attacks against WEP relied on exploiting multiple weak IVs 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 2, the IV and WEP key are hashed to produce a unique packet key (called a temporal key), which is then combined with the IV and XOR'd with the plaintext. The standard 802.11 method of doing the RC4 cryptography in WEP is described in the primer section of this document.

Figure 2 Per Packet WEP Key Hashing



This scenario prevents the weak IVs from being used to derive the base WEP key because the weak IVs allow only you to derive the per-packet WEP key. In order to prevent attacks due to IV collisions, the base key should be changed before the IVs repeat. Since IVs on a busy network can repeat in a matter of hours, mechanisms like LEAP should be used to perform the re-key operation.

Message Integrity Check

Another concern with WEP is its vulnerability to replay attacks. The message integrity check (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.”[1]

[1] Borisov et. al, “Security of the WEP Algorithm”

Summary

Organizations should choose to deploy either IPSec or EAP/802.1X, hereafter referred to as LEAP, but generally not both. Specific designs using both at the same time were tested in the SAFE labs and are discussed in the “Alternatives” sections of the below 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 LEAP. LEAP 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 LEAP is sufficient. Table 1 gives a detailed view of the pros and cons of IPSec and LEAP in WLAN designs:

Table 1 Wireless Encryption Technology Comparison

	LEAP	IPSec	Static WEP
Key Length (bits)	128	168	128
Encryption Algorithm	RC4	3 DES	RC4
Packet Integrity	CRC32/MIC	MD5-HMAC/SHA-HMAC	CRC32/MIC
Device Authentication	None	Pre-shared secret or Certificates	None
User Authentication	Username/Password	Username/Password or OTP	None
User Differentiation *	No	Yes	No
Transparent user experience	Yes	No	Yes
ACL requirements	None	Substantial	N/A
Additional Hardware	Authentication Server	Authentication Server and VPN Gateway	No
Per users keying	Yes	Yes	No
Protocol Support	Any	IP Unicast	Any
Client Support	PCs and high-end PDAs. Wide range of OSs supported from Cisco	PCs and high-end PDAs. Wide range of OSs supported from Cisco and Third-Party Vendors.	All clients supported
Open Standard	No	Yes	Yes
Time-based key rotation	Configurable	Configurable	No
Client hardware Encryption	Yes	Available, software is most common method	Yes
Additional Software	No	IPSec client	No
Per-flow QoS Policy Management	At access switch	After VPN gateway	At access switch

* Described further in “WLAN User Differentiation Challenges” axiom below

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 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

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

Dynamic Host Configuration Protocol

- Requests per second—The 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 LEAP users from gaining IP connectivity after authentication and denying IPSec users from setting up a secure tunnel with the 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 do not group all their DHCP services in one subnet, because a DoS attack against the subnet can deny DHCP service to all wireless users.

RADIUS

- Requests per second—The 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 wireless LANs. If the RADUIS servers are overburdened, wireless access point and VPN gateways will not be able to authenticate users, denying wireless users from gaining 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 wireless LANs.
- Redundant server deployment—Multiple RADIUS servers should be deployed in order to give the authenticating device (wireless access point or VPN gateway) primary and secondary 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 allows 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 synchryonize 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 (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 (IPSec)

- 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 wireless LANs.

- Encryption throughput—The VPN gateway hardware and software must be able to accommodate the projected encryption throughput that will be offered by introducing wireless LANs. 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 wireless LANs. VPN gateways are designed to handle a finite limit of simultaneous IPSec sessions.

Failure to design the IPSec environment with the above 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.

WLAN User Differentiation Challenges

In wired networks, it is often possible to segment users by community through the use of Layer 3 segmentation. In SAFE enterprise, 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 SAFE enterprise, this segmentation can be maintained by filtering on the IP address that the different user communities access. Even in the wired world, this sort of segmentation can be administratively complex because functional and physical separation 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.

Whereas in the wired world this segmentation is difficult but still possible, in the wireless world it becomes nearly impossible with today’s wireless technology. Only by deploying an overlay security mechanism, such as IPSec (discussed previously), can this level of differentiation be achieved. The main problem centers around wireless networks not having physical boundaries within a given location. The financial controller and the guest cubicle in the earlier example will both have access to the same AP.

Because nothing exists today to allow this segmentation, unless you deploy IPSec WLANs, Cisco recommends that you block any system that would normally have Layer 3 controls on its access, based on user community, from access by the wireless network. For example, if you have an R&D system that normally only the developer subnet can access, you should block its use completely in a wireless implementation.

As briefly mentioned earlier, 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 allows for user differentiation and is discussed in detail later in the document.

Design Approach

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/disadvantages of implementing the specific mitigation technologies within SAFE. Any unique characteristics of implementing a mitigation technology within the SAFE designs is also presented. The two main design choices follow:

- Implementing a dynamic WEP keying model using EAP and 802.1X, called LEAP
- Implementing an overlay VPN network using IPSec

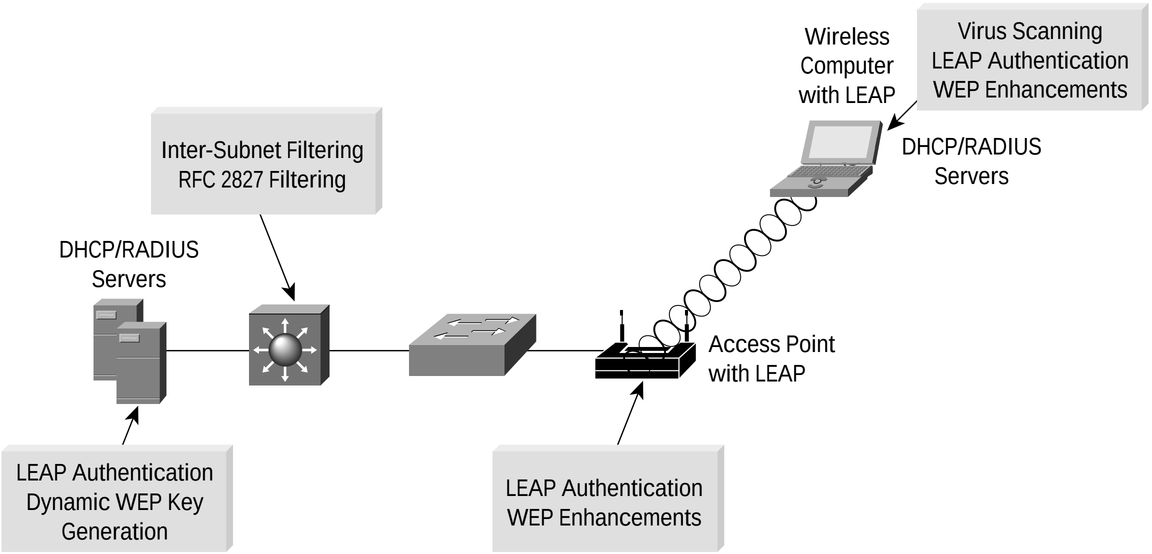
Standard WLAN Design Guidelines

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.

Standard LEAP WLAN Design

This design details a generic method for using LEAP as a security mechanism to access the production corporate network.

Figure 3 Attack Mitigation Roles for Standard LEAP WLAN Design



Key LEAP Devices

- Wireless client adapter and software—A software solution that provides the hardware and software necessary for wireless communications to the AP; it provides mutual authentication to the AP via LEAP
- Wireless access point—Mutually authenticates wireless clients via LEAP
- Layer 2/3 switch—Provides Ethernet connectivity and Layer 3/4 filtering between the WLAN AP and the corporate network
- RADIUS server—Delivers user-based authentication for wireless clients and access-point authentication to the wireless clients
- DHCP server—Delivers IP configuration information for wireless LEAP clients

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 (see "Security Improvements Are Required" axiom), and key rotation using LEAP.
- 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.
- Man in the middle—The mutual authentication nature of LEAP combined with the MIC prevents a hacker from inserting itself 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.
- 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 user's data.
- Network topology discovery—Hackers cannot perform network discovery if they are unable to authenticate. When authenticated via LEAP, standard topology discovery can occur in the same way that is possible in the wired network.

Threats Not Mitigated

- Password attack—Because LEAP does not support one-time passwords (OTPs), the user-authentication process is susceptible to password attacks. The threat can be mitigated by auditing selected passwords for weakness and adhering to a good password usage policy that limits the number of tries for a password before locking out the account.

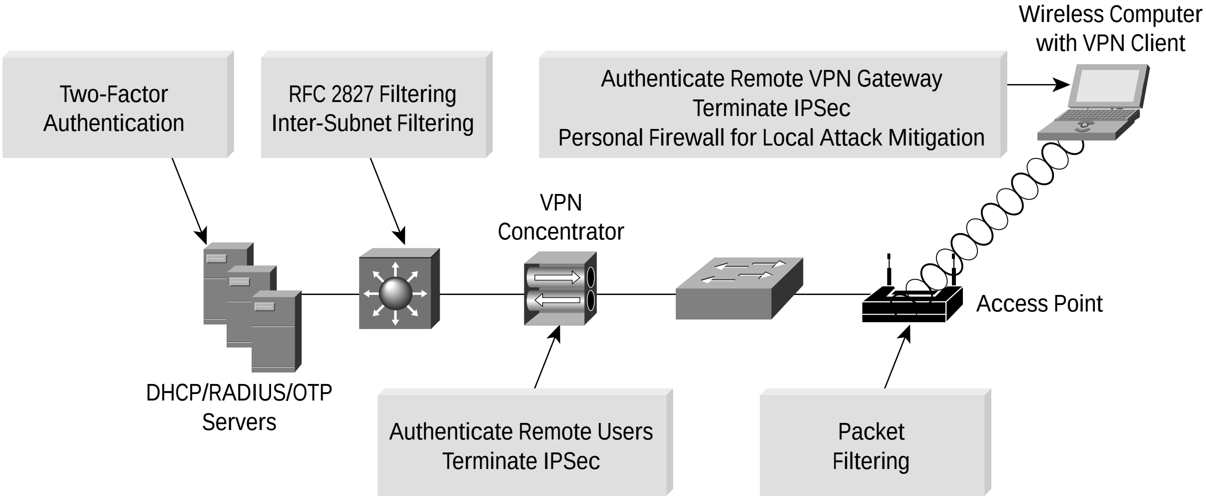
LEAP Design Guidelines

In most cases, WLAN access points are connected to existing Layer 2 access switches. RADIUS and DHCP servers are located in the server module of the corporate network. Security in the design is maintained by preventing network access in the event of a RADIUS service failure. Since 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 APs use LEAP to authenticate the WLAN client devices and end users against the RADIUS servers. Note that because the LEAP process does not support OTP, a significant security hole is introduced into the network because attackers can attempt to brute force the LEAP authentication process. Be sure to require (and check) that users choose strong passwords and set account lockouts after a small number of incorrect login attempts. This configuration can be made at the RADIUS server. 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 LEAP. After successful DHCP configuration, the wireless end user is allowed access to the corporate network. Filtering in place at the first Layer 3 switch prevents the wireless network from accessing portions of the wired network as dictated by an organization's security policy. In SAFE, for example, filtering was put in place to prevent wireless access to any department servers, voice networks, or other user networks. Network designers should give special consideration to the location of the RADIUS and DHCP servers used by LEAP.

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.

Figure 4 Attack Mitigation Roles for Standard VPN WLAN Design


Wireless Computer with VPN Client
Two-Factor Authentication
RFC 2827 Filtering Inter-Subnet Filtering
Authenticate Remote VPN Gateway
Terminate IPSec
Personal Firewall for Local Attack Mitigation
VPN Concentrator
Access Point
DHCP/RADIUS/OTP Servers
Authenticate Remote Users
Terminate IPSec
Packet Filtering

Key VPN Devices

- Wireless client adapter and software—A software solution that provides the hardware and software necessary for wireless communications to the AP
- 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 APs and the corporate network
- 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 one-time password 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

Threats Mitigated

- Wireless packet sniffers—These threats are mitigated by IPSec encryption of wireless client traffic.
- Man in the middle—These threats are mitigated by IPSec encryption 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 AP and Layer 3 switch. Authorization policies can be optionally enforced on the VPN gateway for individual user groups.

- IP spoofing—Hackers can spoof traffic on the wireless LAN, 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.

Threats Not Mitigated

- MAC/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 APs connect to Layer 2 switches in the building module layer on a dedicated VLAN and forward traffic from the WLAN to the wired LAN using IPSec to protect the flows until they reach the wired network. 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 AP 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 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, two mitigation techniques are recommended:

First, the AP 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,and the VPN-specific protocols, IKE (UDP port 500) and ESP (IP Protocol 50). 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.

Secondly, 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.

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).

The VPN gateway can use digital certificates or preshared keys for wireless device authentication. The VPN gateway then takes advantage of OTPs 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.

Alternatives

Network designers may still consider enabling static WEP keys on all devices in an effort to add an additional deterrent against hackers. Although enhancements to WEP such as the MIC and WEP key hashing provide effective risk mitigation to currently identified WEP vulnerabilities, 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.

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 which 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.

Large-Enterprise WLAN Design

The large-enterprise WLAN design overlays wireless LANs 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 below.

Design Guidelines

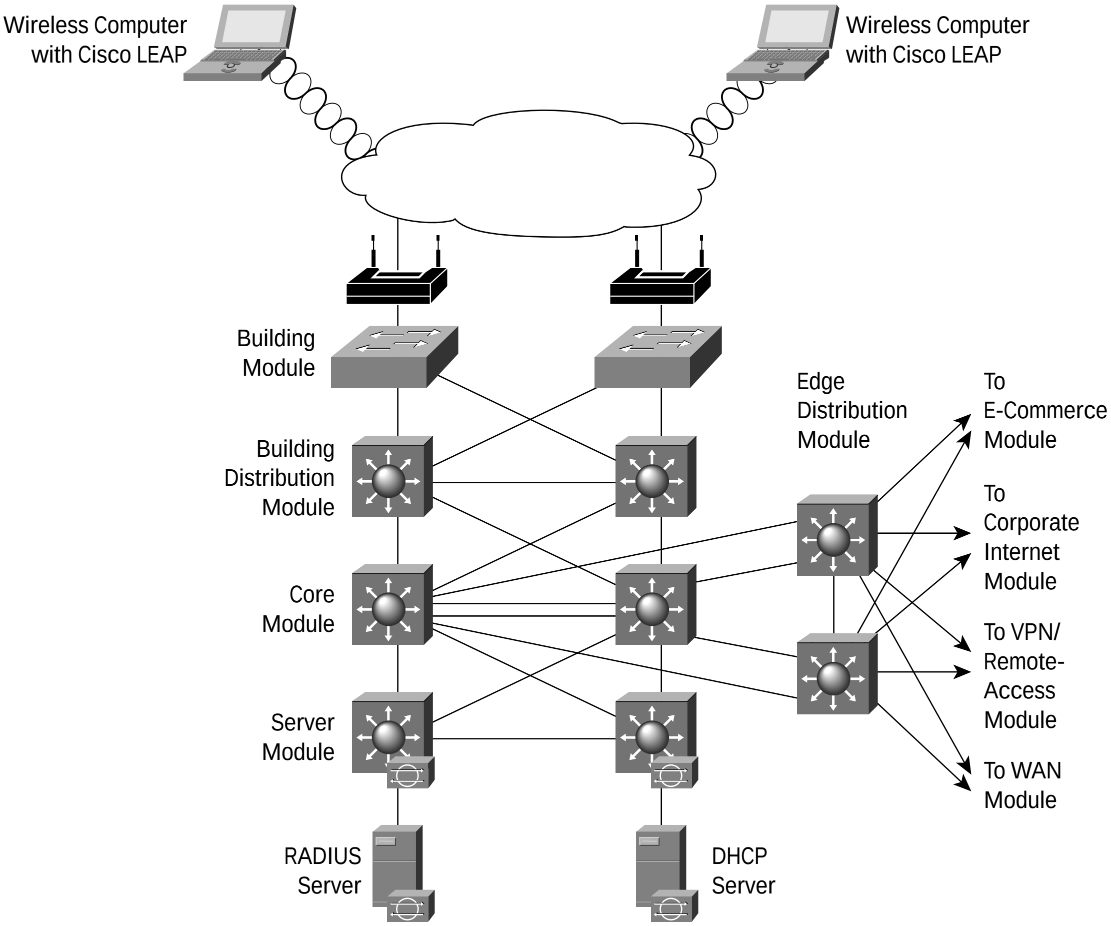
In the large-enterprise WLAN design, scalability and high availability were primary concerns when implementing the mitigation technologies. Both LEAP and VPN are considered viable security options for large-enterprise WLAN designs. Network designers should weigh the business benefits of both technologies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

Network Management

Network management of the AP is restricted to the network management subnet by implementing ACLs in the building distribution Layer 3 switch. Note that because APs support only one wired interface, all management was done in band, versus the out-of-band management as recommended by SAFE enterprise. This setup introduces a security vulnerability into the network because management traffic must be sent in the clear to each AP.

LEAP Option

Figure 5 Large Enterprise LEAP WLAN Design


Wireless Computer with Cisco LEAP
Wireless Computer with Cisco LEAP
Building Module
Building Distribution Module
Core Module
Server Module
RADIUS Server
DHCP Server
Edge Distribution Module
To E-Commerce Module
To Corporate Internet Module
To VPN/ Remote-Access Module
To WAN Module

LEAP access via the wireless network takes advantage of three components from the SAFE enterprise architecture:

- Building module
- Building distribution module
- Server module

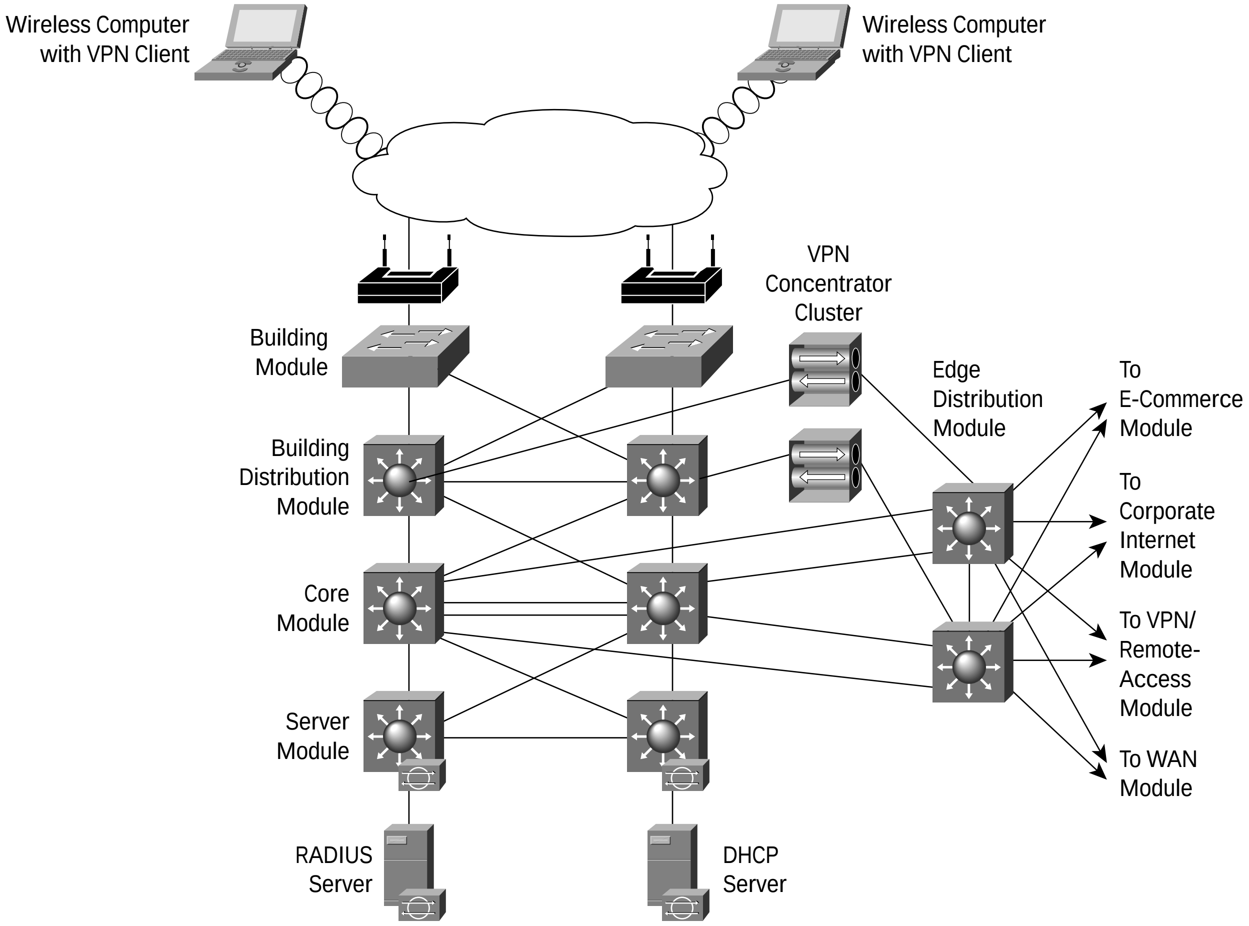
In the large WLAN design, the wireless APs are connected to existing Layer 2 access switches in the building module throughout the corporate campus. RADIUS and DHCP servers are located in the server module. The primary concern for LEAP in a large WLAN design is the availability and scalability of the servers. Following the notes in the axiom section, the RADIUS and DHCP servers are deployed in a redundant fashion on differing network subnets to ensure high availability and scalability. Beyond these notes listed above, the connectivity method is identical to the standard LEAP WLAN design listed above.

Alternatives

When selecting LEAP as the primary security tool for authentication and encryption, the network designer has the option to further enhance the security of the WLAN by creating a policy to limit the access of the wireless clients to only applications requiring a base level of security such as Web browsing. IPSec could then be used in addition to LEAP to allow access to critical business systems (HR, accounting, and so on) after an authorized user authenticates to the VPN gateway. Figure 6 shows IPSec details.

IPSec VPN Option

Figure 6 Large Enterprise VPN WLAN Design


Wireless Computer with VPN Client
Wireless Computer with VPN Client
VPN Concentrator Cluster
Building Module
Building Distribution Module
Edge Distribution Module
To E-Commerce Module
To Corporate Internet Module
Core Module
To VPN/ Remote-Access Module
Server Module
To WAN Module
RADIUS Server
DHCP Server

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 AP 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. In addition to the filters on the AP 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 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 intrusion-detection system (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 the wireless user is associated with. All the above 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 above 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.

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 below.

Design Guidelines

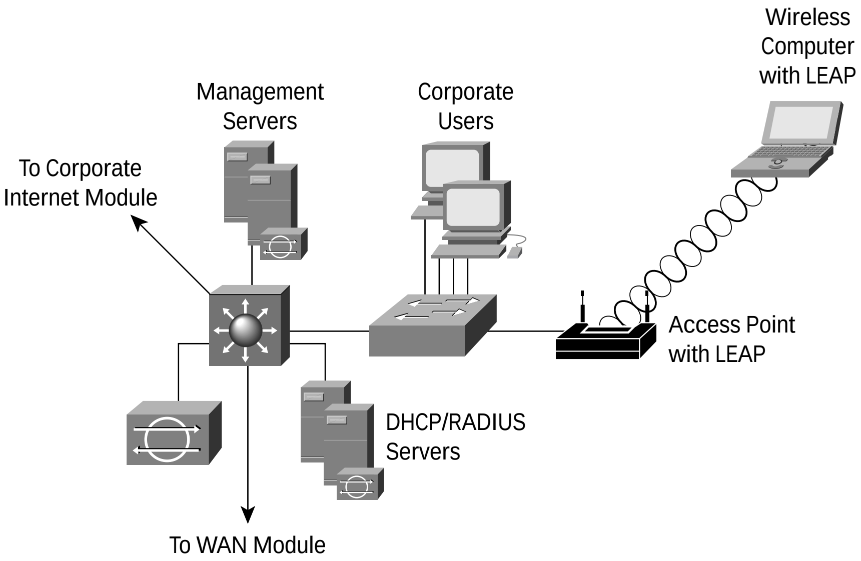
In the medium WLAN design, it is assumed that all WLAN devices are connected to a single IP subnet to enable end-user mobility throughout the medium WLAN design. An assumption is made in the designs that most services available to the medium wired network are also available to the medium WLAN design. Keeping with the design foundation for the SAFE medium network, the medium WLAN design does not offer high availability. Both LEAP and VPN are considered viable security options for a medium WLAN design. Key devices for both the LEAP 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 LEAP 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 the above goals are detailed within each mitigation techniques section.

Network Management

Network management traffic from the management segment to the APs is restricted to the network management subnet by implementing ACLs on the campus Layer 3 switch. Because most APs support only cleartext management protocols (HTTP, SNMP, and so on), encrypted in-band management cannot be done as recommended by the SAFE medium network design. This configuration introduces a security vulnerability into the network because management traffic must be sent in the clear to each AP.

Cisco LEAP Option

Figure 7 Medium Network LEAP WLAN Design



Cisco LEAP access in the medium WLAN design has wireless APs 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 LEAP 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.

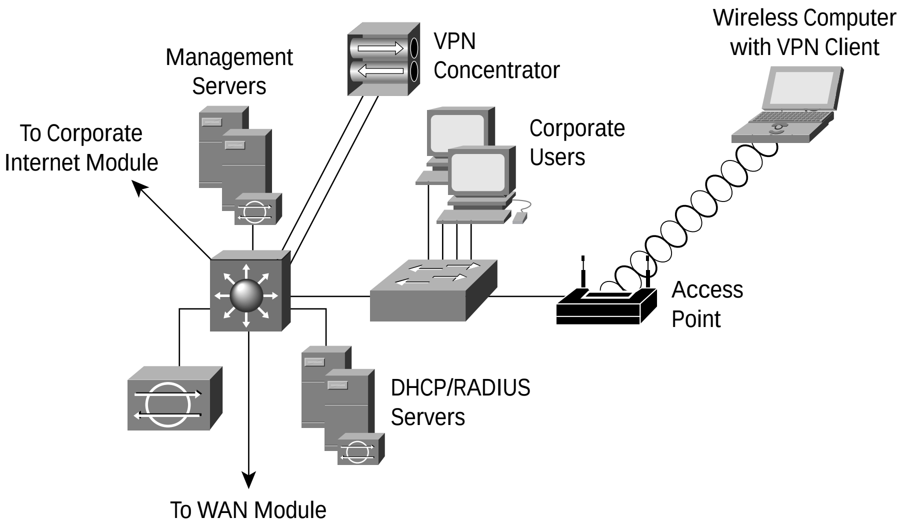
The process of accessing the medium network is the same as outlined in the standard WLAN design guide.

Alternatives

As mentioned in the large LEAP WLAN design, the network designer has the option to further enhance the security of the WLAN by creating a policy to limit the access of the wireless clients to only applications that require a base level of security such as Web browsing. IPSec could then be used in addition to LEAP to allow access to critical business systems. Figure 8 gives IPSec details in a medium WLAN design.

IPSec VPN Option

Figure 8 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. 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 alternatives below 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. The private interface of the VPN gateway connects to a VLAN with access to the wired network. The wireless APs 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 building distribution module Layer 3 switches are configured with ACLs to permit only protocols necessary for VPN connectivity and management.

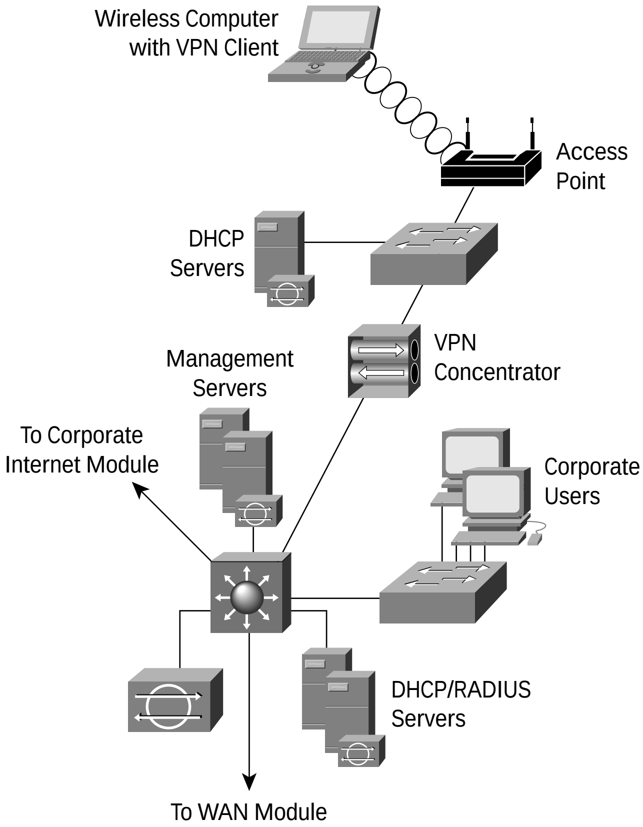
The wireless client establishes an IPSec connection to the wireless VPN gateway. In the process of doing so, the VPN gateway provides device and user authentication via the IPSec VPN. The VPN gateway can use digital certificates or preshared keys for wireless client device authentication. The VPN end 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 the above 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 above design provides 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 9. 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 APs as well as the dedicated DHCP server required for IP configuration of the WLAN client devices.

Figure 9 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, LEAP, 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

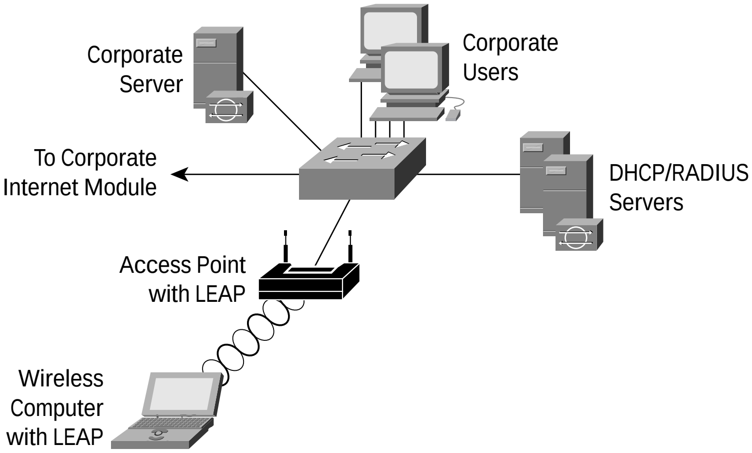
The following sections detail the small WLAN design. Because the small network design has a single Layer 2 switch for its campus connectivity, all devices are assumed to have a single IP subnet network to enable access-point roaming.

Network Management

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

Cisco LEAP Option

Figure 10 Small Network LEAP WLAN Design



Cisco LEAP access in the small WLAN design has wireless APs connected to the existing Layer 2 access switch in the small campus module. The wireless LEAP 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 outlined in the standard WLAN design guide.

Alternatives

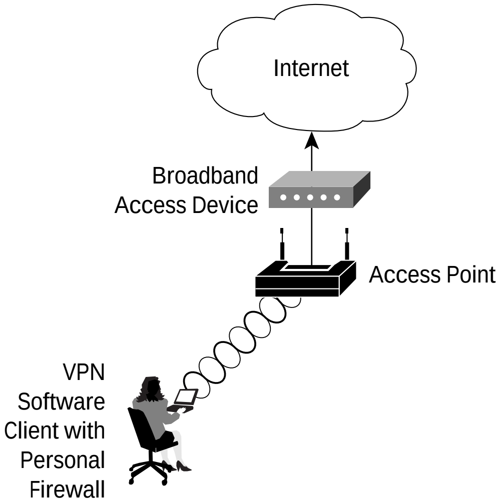
Although not recommended, if an organization is comfortable with managing the key distribution issues, static WEP (with the cryptography fixes listed earlier) can be used as an alternative to LEAP.

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

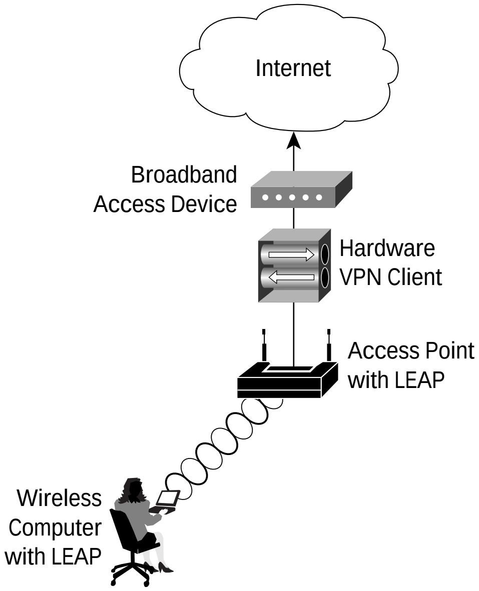
Figure 11 Software VPN Remote Network WLAN Design



The IPSec VPN option in the remote network is recommended when the wireless user requires security from the wireless device to the corporate network. 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 AP 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.

Hardware VPN Remote WLAN Design

Figure 12 Hardware VPN Remote Network WLAN Design



For configurations where an organization's IT department manages VPN and wireless gear at a user's remote location, using LEAP from the PC to the AP and then IPSec from the hardware VPN device to the central office provides a robust security solution for a remote worker. Full-time teleworkers are the most likely individuals to take advantage of this configuration.

When the remote location is using a hardware VPN and LEAP for wireless, the design is nearly identical to 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 AP. 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 AP.

Appendix A: Validation Lab

A reference SAFE 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.

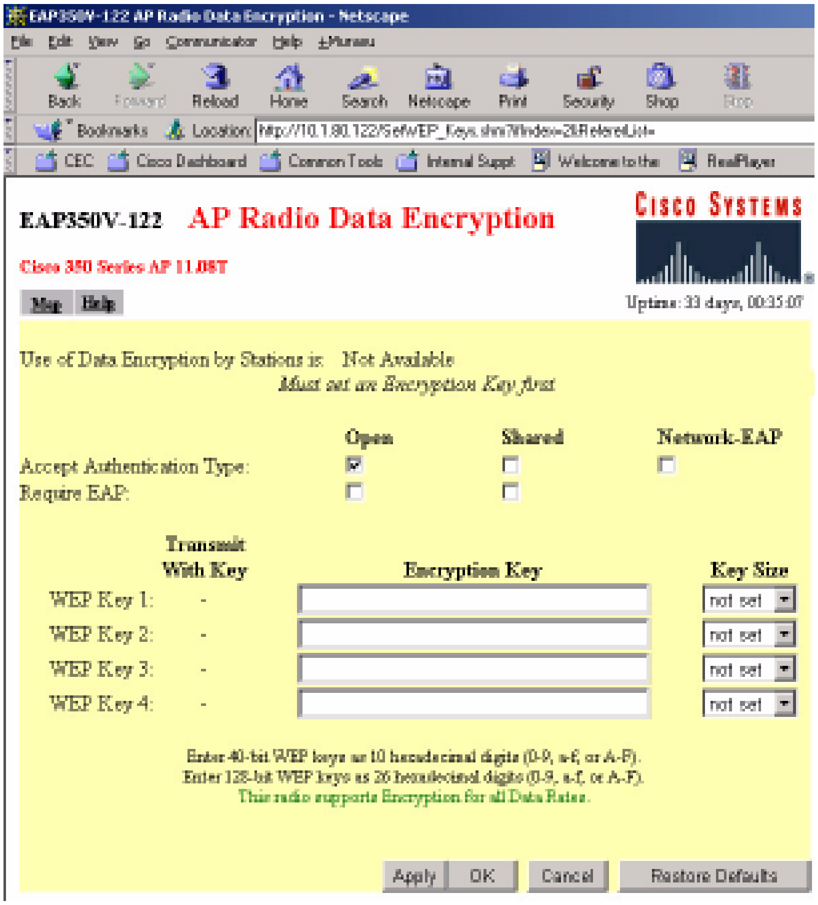
SAFE WLAN Standard Configuration for Access Points

The following sections detail sample configurations needed on APs to enable VPN or LEAP (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. However, configuration for a VPN AP (or a LEAP AP) is identical for all designs.

VPN Access Point

As Figure A-1 illustrates, an AP is configured to allow open authentication, and WEP encryption is not enabled for VPN wireless clients authenticating to a wired network.

Figure A-1: WEP Configuration for a VPN Access Point


EAP350V-122 AP Radio Data Encryption - Netscape
File Edit View Go Communicator Help +Murasu
Back Forward Reload Home Search Netscape Print Security Shop Stop
Bookmarks Location: http://10.1.80.122/SetWEP_Keys.shm?Window=2&ReferedList=
CEC Cisco Dashboard Common Tools Internal Suppt Welcome to the RealPlayer
Cisco Systems
Map Help
Apply OK Cancel Restore Defaults

EAP350V-122 **AP Radio Data Encryption**

Cisco 350 Series AP 11.08T

Uptime: 33 days, 00:35:07

Use of Data Encryption by Stations is: Not Available

Must set an Encryption Key first

	Open	Shared	Network-EAP
Accept Authentication Type:	☑	☐	☐
Require EAP:	☐	☐	

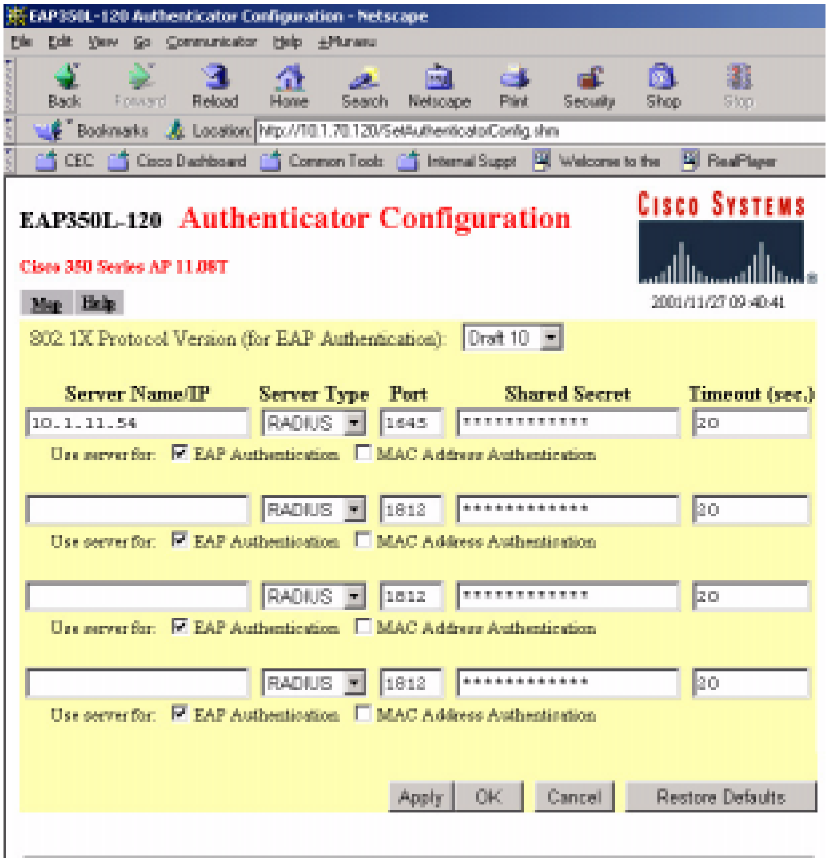
	Transmit With Key	Encryption Key	Key Size
WEP Key 1:	-		not set
WEP Key 2:	-		not set
WEP Key 3:	-		not set
WEP Key 4:	-		not set

Enter 40-bit WEP keys as 10 hexadecimal digits (0-9, a-f, or A-F).
Enter 128-bit WEP keys as 26 hexadecimal digits (0-9, a-f, or A-F).
This radio supports Encryption for all Data Rates.

LEAP Access Point

Figure A-2 shows the Authenticator Configuration window (under Setup >> Security section) on an AP configured to allow LEAP wireless clients to be authenticated by a RADIUS server. It is assumed that either the RADIUS server itself or a network OS server (such as Windows NT server) contains a database of valid users along with passwords.

Figure A-2: Authenticator Configuration Window for a LEAP Access Point


EAP350L-120 Authenticator Configuration - Netscape
File Edit View Go Communicator Help ±Murasu
Back Forward Reload Home Search Netscape Print Security Shop Stop
Bookmarks Location:
CEC Cisco Dashboard Common Tools Internal Suppt Welcome to the RealPlayer
Cisco Systems
Map Help
Apply OK Cancel Restore Defaults

Location: http://10.1.70.120/SetAuthenticatorConfig.shm

EAP350L-120 Authenticator Configuration

Cisco 350 Series AP 11.08T

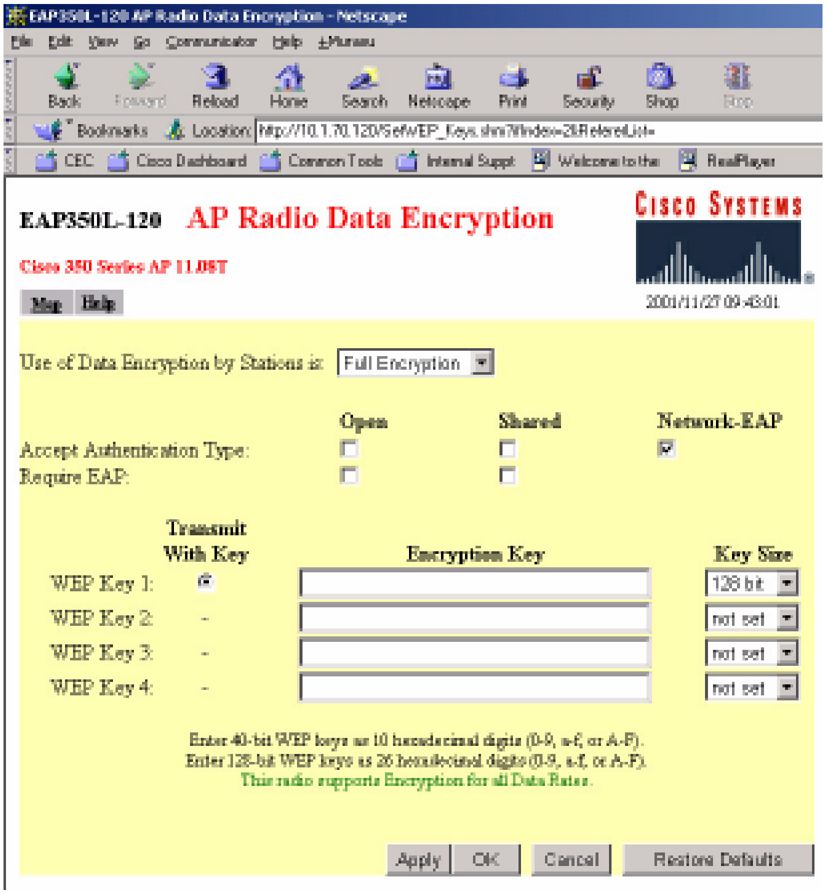
2001/11/27 09:40:41

802.1X Protocol Version (for EAP Authentication): Draft 10

Server Name/IP	Server Type	Port	Shared Secret	Timeout (sec.)
10.1.11.54	RADIUS	1645	*************	20
Use server for: ☑ EAP Authentication ☐ MAC Address Authentication				
	RADIUS	1812	*************	20
Use server for: ☑ EAP Authentication ☐ MAC Address Authentication				
	RADIUS	1812	*************	20
Use server for: ☑ EAP Authentication ☐ MAC Address Authentication				
	RADIUS	1812	*************	20
Use server for: ☑ EAP Authentication ☐ MAC Address Authentication				

Figure A-3 illustrates the WEP configuration for an AP. “Full Encryption” (WEP) is mandated by the AP in addition, the access point allows network EAP as the only authentication method. Furthermore, a 128-bit WEP key (Key 1) is configured for the AP (to be used as a broadcast key).

Figure A-3: WEP Configuration for a LEAP Access Point



EAP350L-120 AP Radio Data Encryption - Netscape
File Edit View Go Communicator Help +Mureau
Back Forward Reload Home Search Netscape Print Security Shop Stop
Bookmarks Location: http://10.1.70.120/SetWEP_Keys.shm?Window=2&RefeedList=
CEC Cisco Dashboard Common Tools Internal Suppt Welcome to the RealPlayer
Cisco Systems
Map Help
Apply OK Cancel Restore Defaults

EAP350L-120 AP Radio Data Encryption

Cisco 350 Series AP 11.08T

2001/11/27 09:43:01

Use of Data Encryption by Stations is: Full Encryption

	Open	Shared	Network-EAP
Accept Authentication Type:	□	□	☑
Require EAP:	□	□	

	Transmit With Key	Encryption Key	Key Size
WEP Key 1:	●		128 bit
WEP Key 2:	-		not set
WEP Key 3:	-		not set
WEP Key 4:	-		not set

Enter 40-bit WEP keys as 10 hexadecimal digits (0-9, a-f, or A-F).
Enter 128-bit WEP keys as 26 hexadecimal digits (0-9, a-f, or A-F).
This radio supports Encryption for all Data Rates.

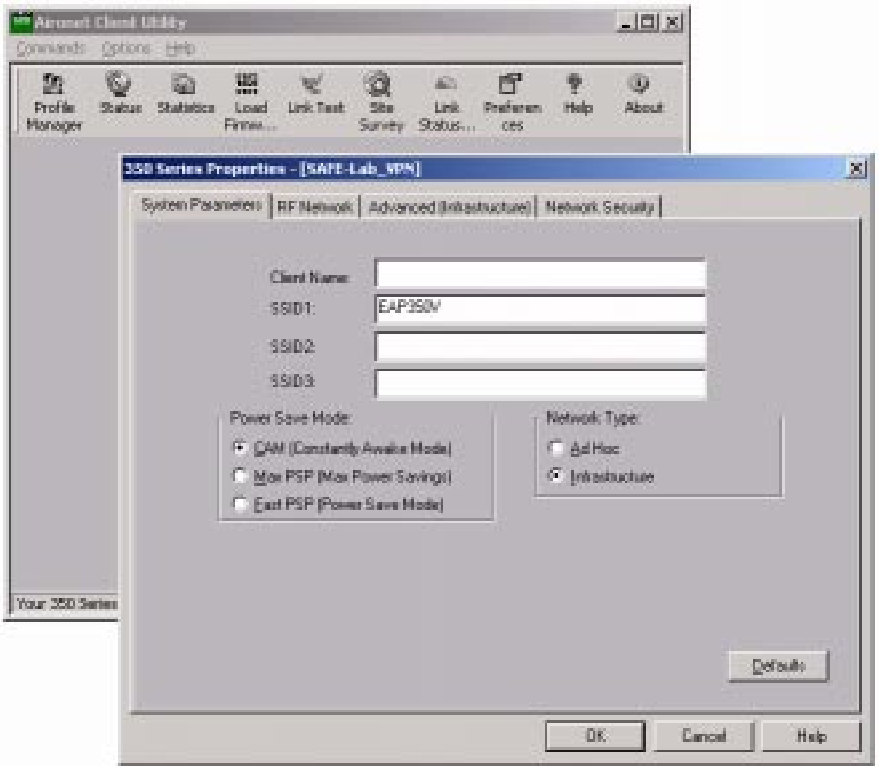
SAFE Wireless LAN Standard Configuration for Clients

The following sections detail sample configurations needed for wireless clients to enable VPN or LEAP (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, WEP and LEAP are disabled on the wireless client. Figures A-4 and A-5 illustrate the sample setup:

Figure A-4: System Parameters Configuration on a VPN Client



Client Name:

SSID1: EAP350V

SSID2:

SSID3:

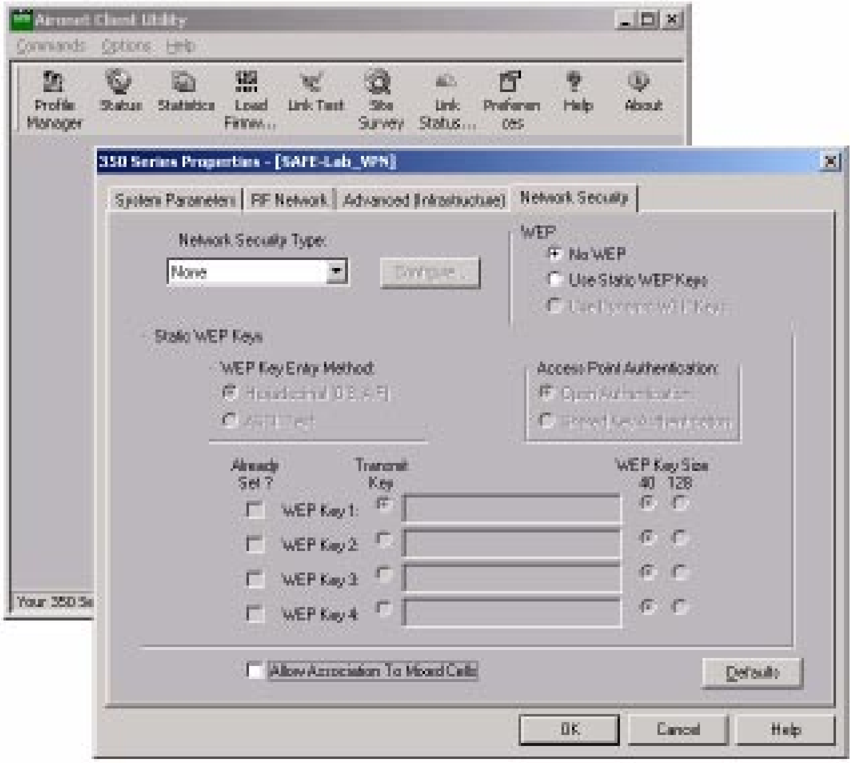
Power Save Mode:

● CAM (Constantly Awake Mode)
○ Max PSP (Max Power Savings)
○ Fast PSP (Power Save Mode)

Network Type:

○ Ad Hoc
● Infrastructure

Figure A-5: Network Security Configuration on a VPN Client



Network Security Type: None

WEP
● No WEP
○ Use Static WEP Keys

As discussed in the Design section of this document, a VPN AP 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 following tables list the inbound (receive) and outbound (transmit) filters to be set on the VPN AP’s radio interface:

Table A-1—VPN AP 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 Port	BootPC	68	Forward
IP Port	DNS	53	Forward
IP Port	IKE	500	Forward

Table A-2—VPN AP 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 Port	BootPS	67	Forward
IP Port	DNS	53	Forward
IP Port	IKE	500	Forward

When creating the above filter sets, be sure to:

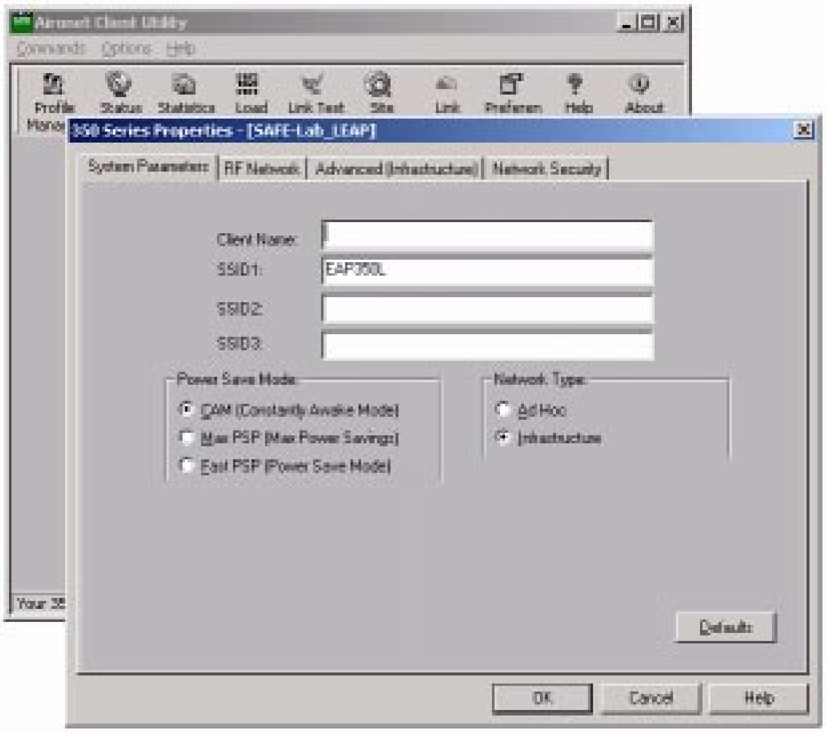
- Set “Default Disposition” of the filter set to “block”
- Enable specific traffic types to flow by adding the specified values (in the above table) to “Special Cases” and select “forward” as the Disposition for each special case

After creating all the filter sets, be sure to apply them to the AP’s radio interface (Setup >> (AP Radio) Filters)

LEAP Client

A wireless client is configured for LEAP by enabling LEAP and WEP using the Aironet® Client utility. Figures A-6, A-7, and A-8 illustrate sample configurations for a LEAP client.

Figure A-6: System Parameters Configuration for a LEAP Wireless Client



350 Series Properties - [SAFE-Lab_LEAP]

Client Name:

SSID1: EAP350L

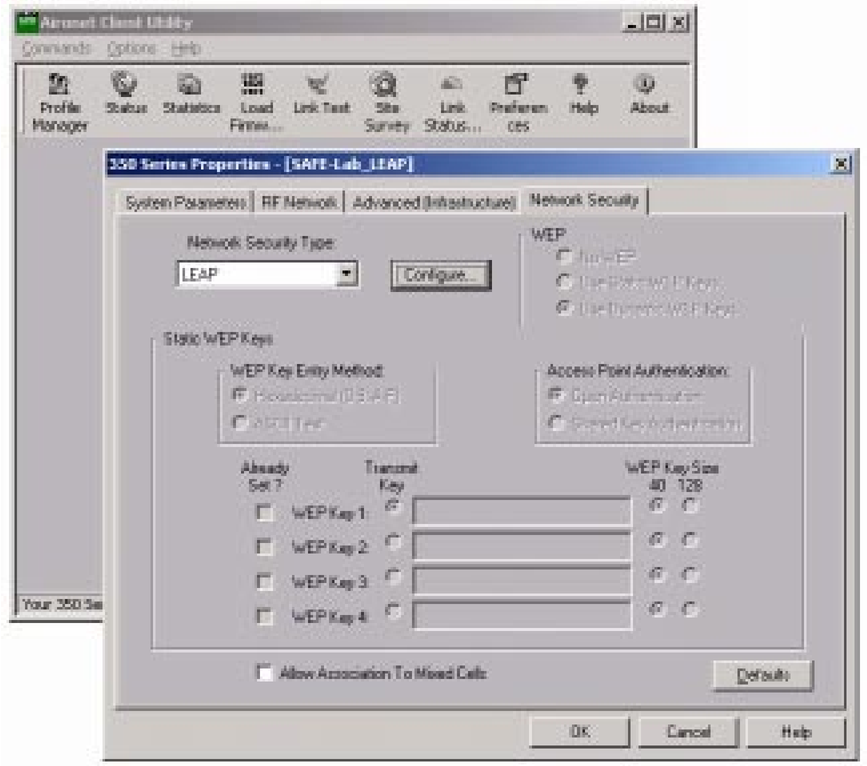
SSID2:

SSID3:

Power Save Mode
- ● CAM (Constantly Awake Mode)
- ○ Max PSP (Max Power Savings)
- ○ Fast PSP (Power Save Mode)

Network Type
- ○ Ad Hoc
- ● Infrastructure

Figure A-7: Network Security Configuration for a LEAP Wireless Client



350 Series Properties - [SAFE-Lab_LEAP]

System Parameters | RF Network | Advanced (Infrastructure) | Network Security

Network Security Type: LEAP | Configure...

WEP
○ No WEP
○ Use Static WEP Keys
● Use Dynamic WEP Keys

Static WEP Keys

WEP Key Entry Method:
● Hexadecimal (0-9, A-F)
○ ASCII Text

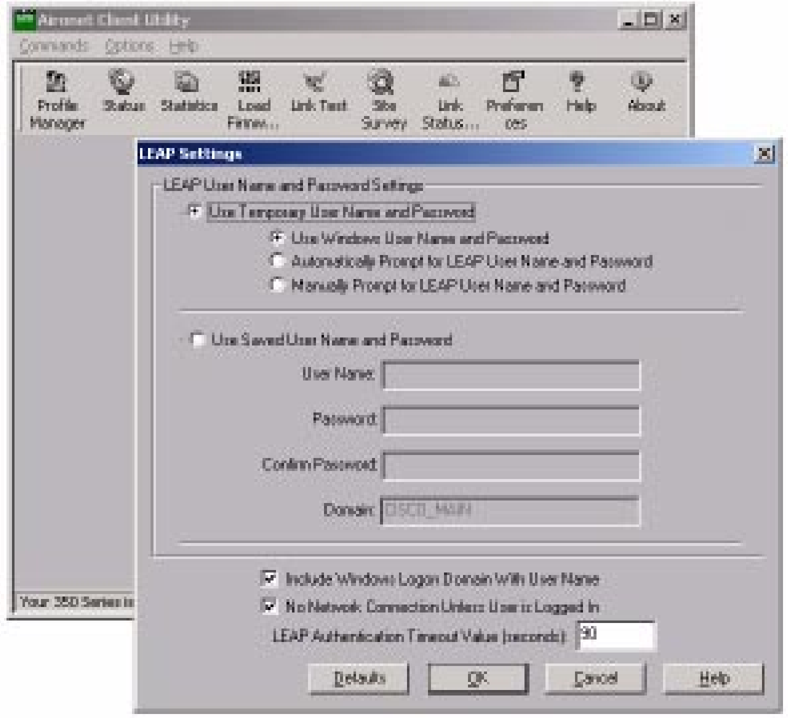
Access Point Authentication:
● Open Authentication
○ Shared Key Authentication

Already Set ?		Transmit Key		WEP Key Size 40	128
□	WEP Key 1:	●		●	○
□	WEP Key 2:	○		●	○
□	WEP Key 3:	○		●	○
□	WEP Key 4:	○		●	○

□ Allow Association To Mixed Cells

Defaults | OK | Cancel | Help

Figure A-8: LEAP Settings Configurations for a LEAP Wireless Client



LEAP Settings

LEAP User Name and Password Settings

● Use Temporary User Name and Password
- ● Use Windows User Name and Password
- ○ Automatically Prompt for LEAP User Name and Password
- ○ Manually Prompt for LEAP User Name and Password

○ Use Saved User Name and Password

User Name:

Password:

Confirm Password:

Domain: CISCO_MAIN

☑ Include Windows Logon Domain With User Name

☑ No Network Connection Unless User is Logged In

LEAP Authentication Timeout Value (seconds): 90

Defaults | OK | Cancel | Help

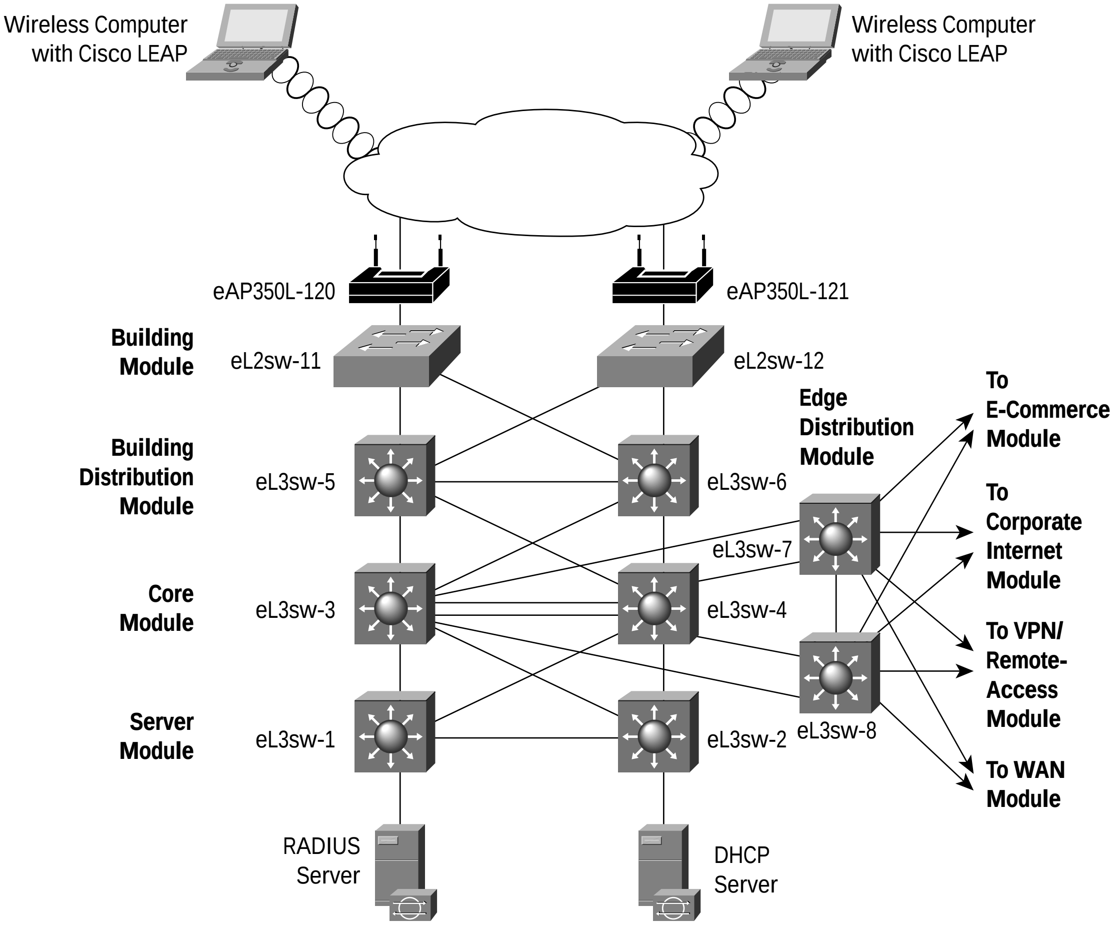
Large-Enterprise Design Module Configurations

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

LEAP Architecture

The following shows a configuration snapshot from the SAFE large-enterprise LEAP WLAN design. Figure A-9 illustrates the LEAP design for a large-enterprise network.

Figure A-9: Large Enterprise LEAP WLAN Design



Products used include the following:

- Cisco Catalyst 6506 Layer 3 Switches (eL3sw-1 to eL3sw-8)
- Cisco Catalyst 4003 Layer 2 Switches (eL2sw-11 to L2sw-12)
- Cisco Aironet 350 Access Points and Clients (eAP350L-120 to 121 and Wireless Clients)
- Cisco Secure Access Control Server (ACS v2.6)
- Windows 2000 DHCP server

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."

eL3sw-5 and eL3sw-6 (WLAN building module to building-distribution module interconnection):

```
! APs are placed on an independent VLAN 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

! Deny all traffic from clients behind APs to clients on protected wired segments
access-list 170 deny ip 10.1.70.0 0.0.0.255 10.1.5.0 0.0.0.255 log
access-list 170 deny ip 10.1.70.0 0.0.0.255 10.1.6.0 0.0.0.255 log
access-list 170 deny ip 10.1.70.0 0.0.0.255 10.1.7.0 0.0.0.255 log
access-list 170 deny ip 10.1.70.0 0.0.0.255 10.1.8.0 0.0.0.255 log
access-list 170 deny ip 10.1.70.0 0.0.0.255 10.1.15.0 0.0.0.255 log
access-list 170 deny ip 10.1.70.0 0.0.0.255 10.1.16.0 0.0.0.255 log
access-list 170 deny ip 10.1.70.0 0.0.0.255 10.1.80.0 0.0.0.255 log

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

! Permit traffic from users with valid IP addresses and deny all others
access-list 170 permit ip 10.1.70.0 0.0.0.255 any
access-list 170 deny ip any any log

! Deny all traffic from protected wired subnets to wireless clients
access-list 171 deny ip 10.1.5.0 0.0.0.255 10.1.70.0 0.0.0.255 log
access-list 171 deny ip 10.1.6.0 0.0.0.255 10.1.70.0 0.0.0.255 log
access-list 171 deny ip 10.1.7.0 0.0.0.255 10.1.70.0 0.0.0.255 log
access-list 171 deny ip 10.1.8.0 0.0.0.255 10.1.70.0 0.0.0.255 log
access-list 171 deny ip 10.1.15.0 0.0.0.255 10.1.70.0 0.0.0.255 log
access-list 171 deny ip 10.1.16.0 0.0.0.255 10.1.70.0 0.0.0.255 log
access-list 171 deny ip 10.1.70.0 0.0.0.255 10.1.70.0 0.0.0.255 log
access-list 171 deny ip 10.1.80.0 0.0.0.255 10.1.70.0 0.0.0.255 log

! Permit outgoing web traffic to the 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

! Permit RADIUS responses from the AAA Server
access-list 171 permit udp host 10.1.11.54 eq 1645 host 10.1.70.120 gt 1023
access-list 171 permit udp host 10.1.11.54 eq 1645 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

! Permit all IP traffic from the wired network to the wireless network
access-list 171 permit ip any 10.1.70.0 0.0.0.255
access-list 171 deny ip any any log
```

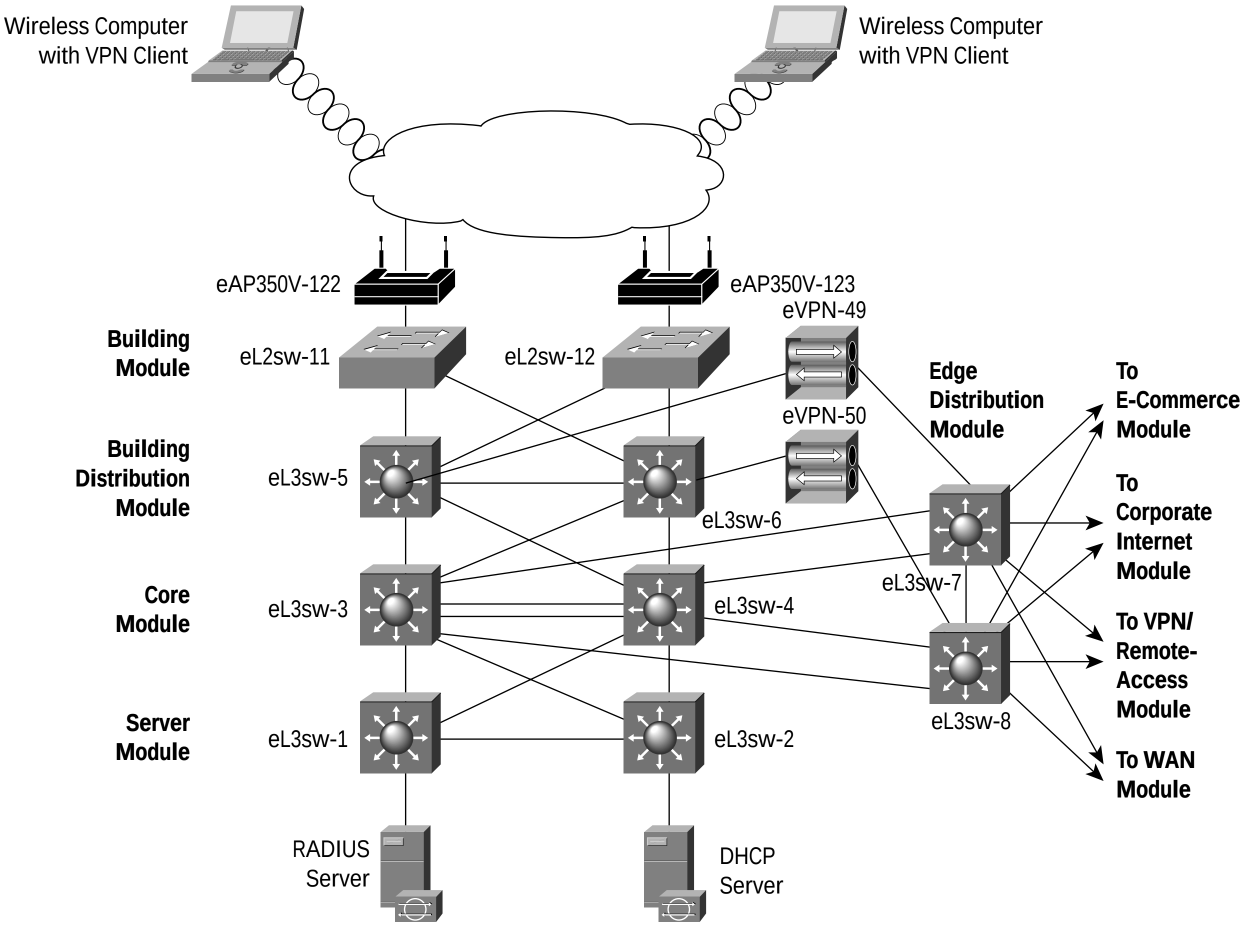
eAP350L-120 to 121 and Wireless Clients:

Refer to the configuration samples in the "Overall Guidelines" section of this appendix for configuring an AP and wireless client for LEAP.

VPN Architecture

The following shows a configuration snapshot from the SAFE large-enterprise VPN WLAN design. Figure A-10 illustrates the VPN design for a WLAN in a large enterprise.

Figure A-10: Large Enterprise VPN WLAN Design



Products used include the following:

- Cisco Catalyst 6506 Layer 3 Switches (eL3sw-1 to eL3sw-8)
- Cisco Catalyst 4003 Layer 2 Switches (eL2sw-9 to eL2sw-14)
- Cisco VPN 3015 Concentrator (eVPN-49 to 50)
- Cisco Aironet 350 Access Points and Clients (eAP350V-122 to 123 and Wireless Clients)
- Cisco Secure Access Control Server (ACS v2.6)
- Windows 2000 DHCP server
- Cisco IDS Host Sensor

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.”

eL3sw-5 and eL3sw-6 (WLAN building module to building distribution module interconnection):

```
! APs are placed on an independent VLAN 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

! Permit IPSec traffic to the VPN gateway subnet
access-list 180 permit esp 10.1.80.0 0.0.0.255 10.1.50.0 0.0.0.255
access-list 180 permit udp 10.1.80.0 0.0.0.255 eq isakmp 10.1.50.0 0.0.0.255 eq isakmp

! Permit Full ICMP for troubleshooting
access-list 180 permit icmp 10.1.80.0 0.0.0.255 10.1.50.0 0.0.0.255
access-list 180 permit icmp 10.1.80.0 0.0.0.255 host 10.1.80.5

! Permit DHCP requests for the initial IP assignment for the wireless client
access-list 180 permit udp host 0.0.0.0 eq bootpc host 255.255.255.255 eq bootps
access-list 180 permit udp 10.1.80.0 0.0.0.255 eq bootpc host 255.255.255.255 eq bootps
access-list 180 permit udp 10.1.80.0 0.0.0.255 eq bootpc host 10.1.11.50 eq bootps

! Permit web responses from the APs for management
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

! Deny all other traffic, don’t log Windows file share broadcasts
access-list 180 deny udp 10.1.80.0 0.0.0.255 any eq netbios-ns
access-list 180 deny udp 10.1.80.0 0.0.0.255 any eq netbios-dgm
access-list 180 deny ip any any log

! Permit IPSec traffic to the wireless subnet
access-list 181 permit esp 10.1.50.0 0.0.0.255 10.1.80.0 0.0.0.255
access-list 181 permit udp 10.1.50.0 0.0.0.255 eq isakmp 10.1.80.0 0.0.0.255 eq isakmp

! Permit Full ICMP for troubleshooting
access-list 181 permit icmp 10.1.50.0 0.0.0.255 10.1.80.0 0.0.0.255

! Permit DHCP responses for the initial IP assignment for the wireless client
access-list 181 permit udp host 10.1.11.50 eq bootps host 255.255.255.255 eq bootpc
access-list 181 permit udp host 10.1.11.50 eq bootps 10.1.80.0 0.0.0.255 eq bootpc

! Permit incoming web requests to the APs for management
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

! Deny all other traffic
access-list 181 deny ip any any log
```

eAP350V-122 to 123 and Wireless Clients

Refer to the configuration samples in the “Overall Guidelines” section of this appendix for configuring APs and wireless clients for VPN connectivity over a WLAN.

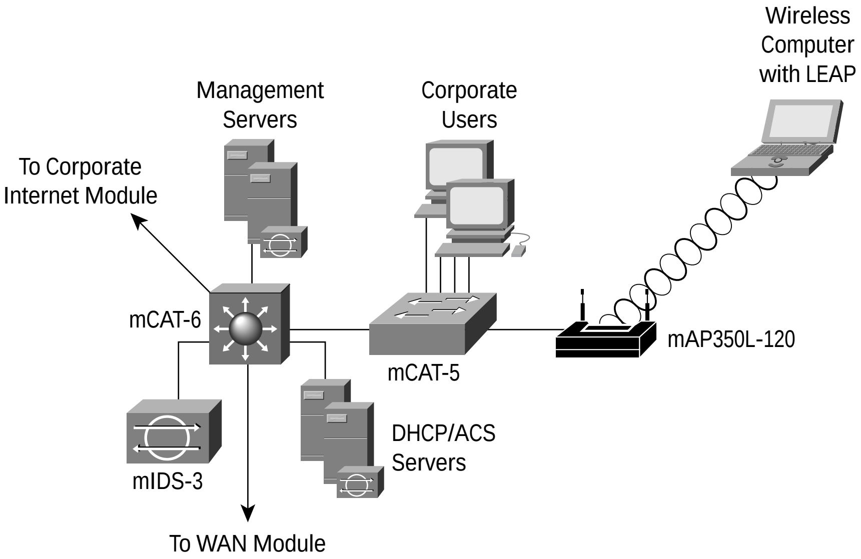
Medium Network Configurations

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

LEAP Architecture

The following shows a configuration snapshot from the SAFE medium-enterprise WLAN design with LEAP option. Figure A-11 illustrates the LEAP WLAN design for a medium-enterprise network.

Figure A-11: Medium LEAP WLAN Design



Products used include the following:

- Cisco Catalyst Layer 3 Switch (mCAT-6)
- Cisco Catalyst Layer 2 Switch (mCAT-5)
- Cisco Aironet Access Point and Client (mAP350L-120 and Wireless Client)
- Cisco Secure Access Control Server (ACS v2.6)
- Windows 2000 DHCP server

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

MCAT-6:

```
! APs are placed in an independent VLAN in the Medium Enterprise Network
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

! Deny all traffic from clients behind APs to clients on protected wired segments
access-list 170 deny ip 10.3.70.0 0.0.0.255 10.3.1.0 0.0.0.255

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

! Permit traffic from users with valid IP addresses and deny all others
access-list 170 permit ip 10.3.70.0 0.0.0.255 any
access-list 170 deny ip any any log

! Deny all traffic from protected wired subnets to wireless clients
access-list 171 deny ip 10.3.1.0 0.0.0.255 10.3.70.0 0.0.0.255 log
access-list 171 deny ip 10.3.70.0 0.0.0.255 10.3.70.0 0.0.0.255 log
access-list 171 deny ip 10.3.80.0 0.0.0.255 10.3.70.0 0.0.0.255 log

! Permit outgoing web traffic to the APs for management
access-list 171 permit tcp 10.3.8.0 0.0.0.255 gt 1023 host 10.3.70.120 eq www

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

! Deny all other IP traffic to APs
access-list 171 deny ip any host 10.3.70.120 log

! Permit all IP traffic from the wired network to the wireless network
access-list 171 permit ip any 10.3.70.0 0.0.0.255
```

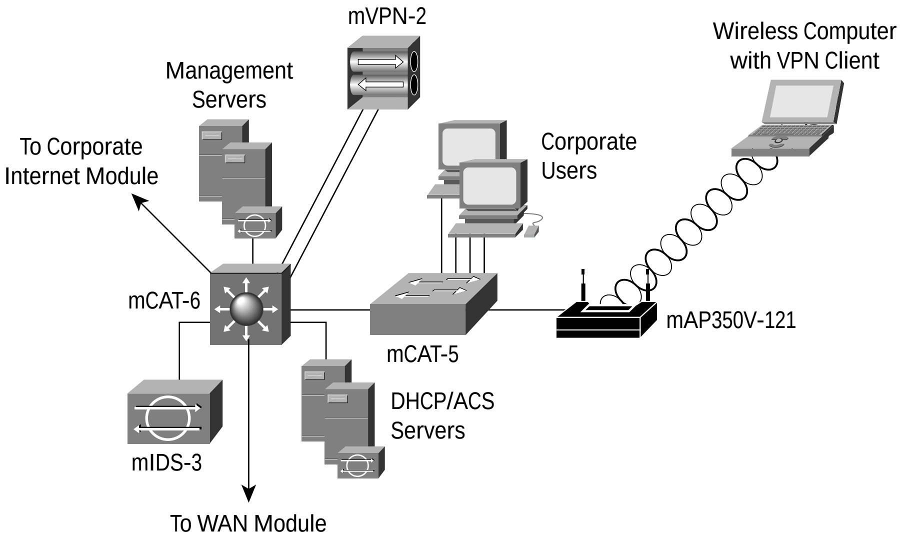
mAP350L-120 and Wireless Client:

Refer to the configuration samples in the “Overall Guidelines” section of this appendix for configuring APs and wireless clients for the LEAP option.

VPN Architecture

The following shows a configuration snapshot from the SAFE medium WLAN design with VPN option. Figure A-12 illustrates the VPN WLAN design for a medium network.

Figure A-12: Medium VPN WLAN Design



Products used include the following:

- Cisco Catalyst Layer 3 Switch (mCAT-6)
- Cisco Catalyst Layer 2 Switch (mCAT-5)
- Cisco Aironet Access Point and Client (mAP350V-121 and Wireless Client)
- Cisco VPN 3000 series concentrator (mVPN-2)
- Cisco Secure Access Control Server (ACS v2.6)
- Windows 2000 DHCP server
- Cisco IDS Host Sensor

MCAT-6:

```
! APs are placed on an independent VLAN in the campus network
interface Vlan80
 ip address 10.3.80.1 255.255.255.0
 ip access-group 180 in
 ip access-group 181 out
 ip helper-address 10.3.2.50
 no ip redirects
 no cdp enable

! Permit web responses from the APs for management
access-list 180 permit tcp host 10.3.80.121 eq www 10.3.8.0 0.0.0.255 gt 1023 established

! Permit IPSec traffic to the VPN gateway subnet
access-list 180 permit esp 10.3.80.0 0.0.0.255 10.3.16.0 0.0.0.255
access-list 180 permit udp 10.3.80.0 0.0.0.255 eq isakmp 10.3.16.0 0.0.0.255 eq isakmp

! Permit Full ICMP for troubleshooting
access-list 180 permit icmp 10.3.80.0 0.0.0.255 10.3.16.0 0.0.0.255
access-list 180 permit icmp 10.3.80.0 0.0.0.255 host 10.3.80.1

! Permit DHCP requests for the initial IP assignment for the wireless client
access-list 180 permit udp host 0.0.0.0 eq bootpc host 255.255.255.255 eq bootps
access-list 180 permit udp 10.3.80.0 0.0.0.255 eq bootpc host 255.255.255.255 eq bootps
access-list 180 permit udp 10.3.80.0 0.0.0.255 eq bootpc host 10.3.2.50 eq bootps

! Deny all other traffic, don’t log Windows file share broadcasts
access-list 180 deny udp 10.3.80.0 0.0.0.255 any eq netbios-ns
access-list 180 deny udp 10.3.80.0 0.0.0.255 any eq netbios-dgm
access-list 180 deny ip any any log

! Permit IPSec traffic to the wireless subnet
access-list 181 permit esp 10.3.16.0 0.0.0.255 10.3.80.0 0.0.0.255
access-list 181 permit udp 10.3.16.0 0.0.0.255 eq isakmp 10.3.80.0 0.0.0.255 eq isakmp

! Permit Full ICMP for troubleshooting
access-list 181 permit icmp 10.3.16.0 0.0.0.255 10.3.80.0 0.0.0.255

! Permit DHCP responses for the initial IP assignment for the wireless client
access-list 181 permit udp host 10.3.2.50 eq bootps host 255.255.255.255 eq bootpc
access-list 181 permit udp host 10.3.2.50 eq bootps 10.3.80.0 0.0.0.255 eq bootpc

! Permit incoming web requests to the APs for management
access-list 181 permit tcp 10.3.8.0 0.0.0.255 gt 1023 host 10.3.80.121 eq www

! Deny all other traffic
access-list 181 deny ip any any log
```

mAP350V-121 and Wireless Client:

Refer to the configuration samples in the “Overall Guidelines” section of this appendix for configuring APs and wireless clients for the VPN option.

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. It can 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 AP. 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. 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 Wireless Ethernet Compatibility Alliance (WECA) provides a branding for 802.11-based technology known as Wi-Fi. A Wi-Fi-compliant device must pass interoperability testing in the WECA laboratory, and it provides a guarantee to the users that their equipment will work with all other Wi-Fi-certified vendors.

Standard 802.11-based wireless technologies take advantage of the radio spectrum deemed usable by the public. This spectrum is known as the ISM band, or Industrial, Scientific, and Medical 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 it 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. A common primary owner of the 2.4-GHz band are 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 600 W). With spread-spectrum technology, if there is ever any overlap with the primary owner, the primary owner has what can effectively be called ‘RF right of way.’

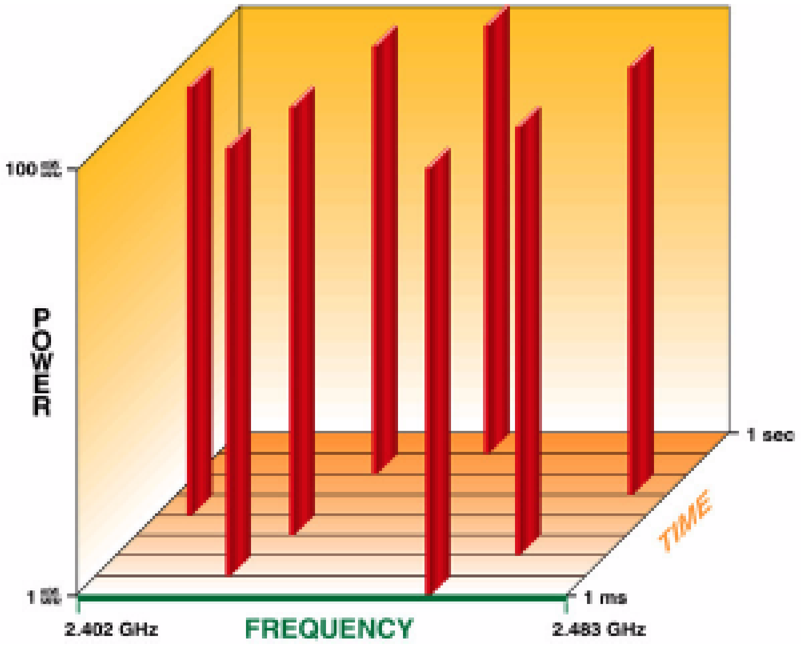
The 802.11 standard specifies two different types of Layer 1 physical interfaces for radio-based devices. One uses a frequency-hopping architecture, whereas the other uses a more straightforward single-frequency approach, known as direct sequencing.

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.

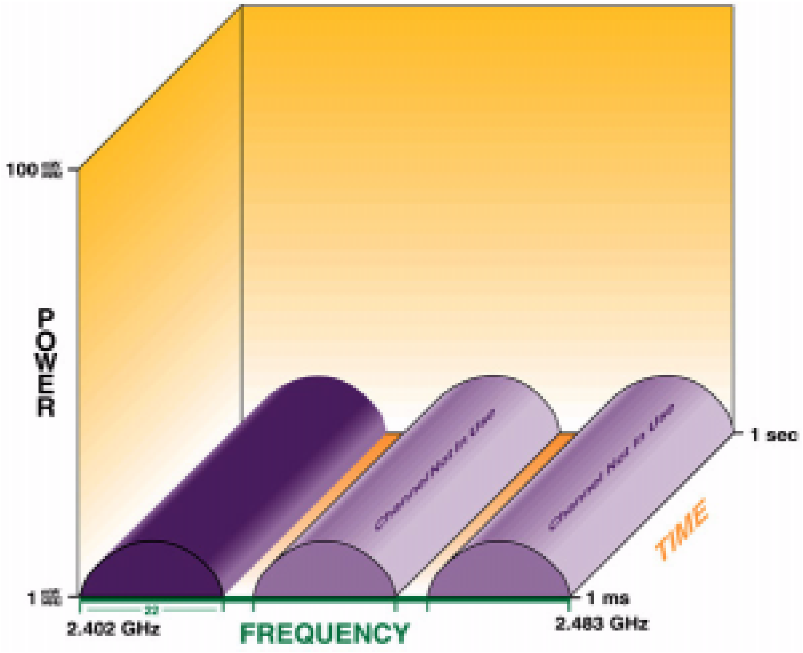
Figure B-1: Frequency Hopping



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 three 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 APs 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 frequency-division multiplexing (OFDM). In a FDM system, the available bandwidth is divided into multiple data carriers. The data to be transmitted is then divided between 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 chunks, 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. 802.3 relies on upper-layer protocols to deal with frame retransmission.

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 acknowledgement function to provide notifications to the sender that the destination has received the frame. For every frame transmitted, the receiving station responds with an acknowledgement (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 they are associated to. 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.

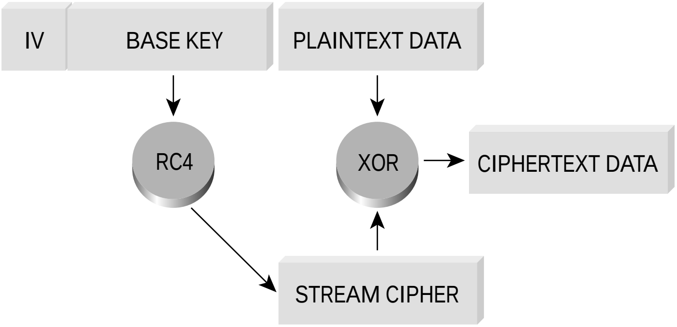
Frame Encryption

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/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/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/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 (IV) to be concatenated with the symmetric key before generating the stream ciphertext.

The IV is a 24-bit value (ranging from 0 to 16777215). The IEEE suggests—but does not mandate—that the IV change per frame. Because the sender generates the IV 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 IV 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 IV 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 (APs), Network Interface Cards (NICs)/client adapters, bridges, and antennas.

Access point—An AP 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 AP also coordinates the wireless clients' use of wired resources.

Network interface card (NIC)/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/workstation operating system 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 APs (IEEE 802.11 standard specifies 1 mile as the maximum coverage range for an AP).

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 AP/bridge and the clients.

References

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

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 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/

Acknowledgements

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 Andy Balinsky, Bruce McMurdo, Brian Cox, and Roland Saville. Thank you all for your special effort.

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems Europe
11, Rue Camille Desmoulins
92782 Issy-les-Moulineaux
Cedex 9
France
www-europe.cisco.com
Tel: 33 1 58 04 60 00
Fax: 33 1 58 04 61 00

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 317 7777
Fax: +65 317 7799

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

LW2878 12/01

Printed in the USA