On completing this chapter, you will be able to

- Explain the different WLAN configurations
- Explain how WLANs work
- Describe the risks of open wireless ports
- Describe SAFE WLAN design techniques

CHAPTER 14

Wireless Security

This chapter covers wireless security—what it is, how it works, how it is configured, what threatens it, and what policies can be designed to secure it. Wireless networking has limitations, involves some risks, and requires defense techniques, as you learn in this chapter. All network architectures, including the wireless networking sector of an organization's network, should be based on sound security policies. These policies are designed to address all the weaknesses and threats that can occur in today's large, wireless TCP/IP-based networks.

There is no doubt that mobile computing is booming. Users want to keep their mobile devices connected to the network at all times so that productivity is no longer limited to areas where a physical network connection is located. Users can now move from place to place, computing when and where they want. This section should help you understand the basics of wireless local-area networks (WLANs) networking. WLANs are defined by the Institute of Electrical and Electronics Engineers (IEEE) organization with the 802.11 standard for wireless Ethernet. Standard WLANs that are based on the 802.11 IEEE standards provide mobility to corporate network users while maintaining access to network resources at all times and locations within the building or campus.

NOTE The IEEE has established the IEEE 802.11 standard, which is the predominant standard for WLANs. IEEE standards can be downloaded at the following location: http://standards.ieee.org/.

Laptops connected to the wireless network are becoming the primary computing devices in the workplace, providing users with the advantage of much greater flexibility in meetings, conferences, and during business travel. Companies and organizations offering this type of network connectivity in venues previously unavailable will indisputably generate a higher productivity per employee because critical business information is available at any time and place during the business day. Furthermore, this technology is a solution for areas that are difficult to wire, such as older buildings with complex infrastructures and obstacles. In the United States, there are many homes and buildings on the National Historic Register (mostly older structures, some developed by famous modern architects). It is illegal to

modify these buildings, which often includes running cables in walls. To comply with legal restrictions, networking these buildings can involve taping wires to the baseboards. Wireless networking is a happy solution for those who work and live in such buildings.

Different WLAN Configurations

As you will see in the case study at the end of the chapter, wireless network connectivity is not limited to corporate enterprise buildings. WLANs also offer connectivity outside the traditional office environment. Numerous wireless Internet service providers are appearing in airports (hotspots), trains, hotels, and conference and convention centers.

As with most technologies, the early wireless networks were nonstandard, and only vendor-proprietary technologies existed. This caused interoperability issues between the different standards of WLAN technologies with vendor-specific implementations. Standards-based WLAN technologies were developed because of the interoperability issues. Today, several standards exist for WLAN applications: 802.11, HiperLAN, HomeRF Shared Wireless Access Protocol, and Bluetooth. This chapter focuses on the 802.11 implementations, which are the most widely used.

For an end user, WLANs can be categorized as follows:

- Peer-to-peer
- LAN
- Hotspots

For a network administrator, WLANs can be categorized as follows:

- Point-to-point bridge
- Point-to-multipoint bridge
- Ethernet to wireless bridge

One of the earliest setups for WLANs was in peer-to-peer WLAN configurations. Wireless clients equipped with wireless network interface cards (NICs) communicate with each other without the use of an independent network device called an access point. These wireless NICs exist in different types: card bus, Personal Computer Memory Card International Association (PCMCIA), and Peripheral Component Interconnect (PCI). Peer-to-peer LANS have limitations such as limited coverage area and lack of access to wired resources.

NOTE Among the first wireless devices were laptops with built-in infrared ports. Many peer-to-peer transfers were accomplished successfully over these ports to replace null modem cable transfers. Now Ethernet crossover cables accomplish this purpose.

Figure 14-1 illustrates the peer-to-peer WLAN configuration.

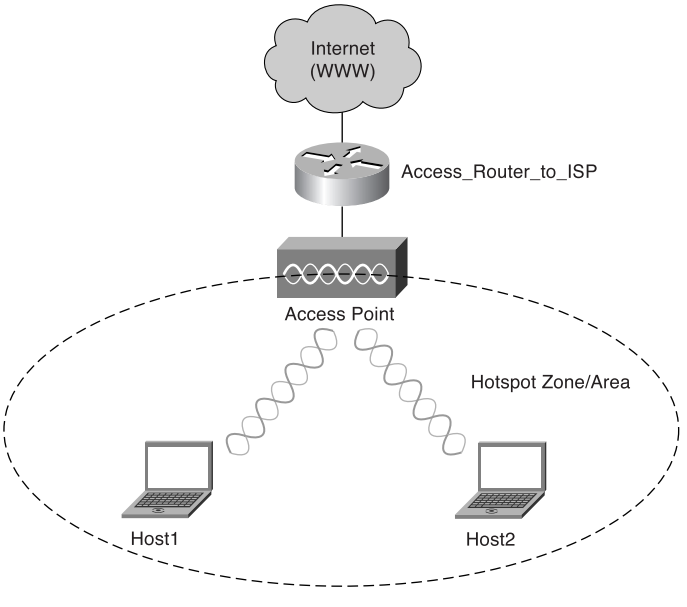
Figure 14-1 *Peer-to-Peer WLAN*

The peer-to-peer WLAN is often referred to as the independent basic service set (IBSS), as discussed later in the chapter.

A multiple-segment WLAN extends the coverage of a peer-to-peer WLAN through the use of overlapping zones or areas. The coverage area of a zone is determined by the characteristics of the access point (a wireless bridge) that coordinates the wireless clients' use of wired resources.

Typical examples of these zones are hotspots in airports, coffee shops, and hotels. Your hotel provides access in the room, in the restaurant, in the lobby, and in the conference rooms. You are able to roam about without losing the connection. Figure 14-2 shows the setup of a wireless hotspot.

Figure 14-2 *Hotspot WLAN*



The hotspot WLAN is often referred to as the infrastructure basic service set.

NOTE An extension of these hotspots is found in community networks. These types of networks extend Internet access with free access. The purchase, installation, and maintenance are taken care of by the community. Community networks can extend to include schools, neighborhoods, and small businesses. It has been noted recently that community networks are not limited to certain areas; instead, wireless community networks are popping up worldwide.

A full database of worldwide deployments of wireless community networks can be found at http://www.nodedb.com.

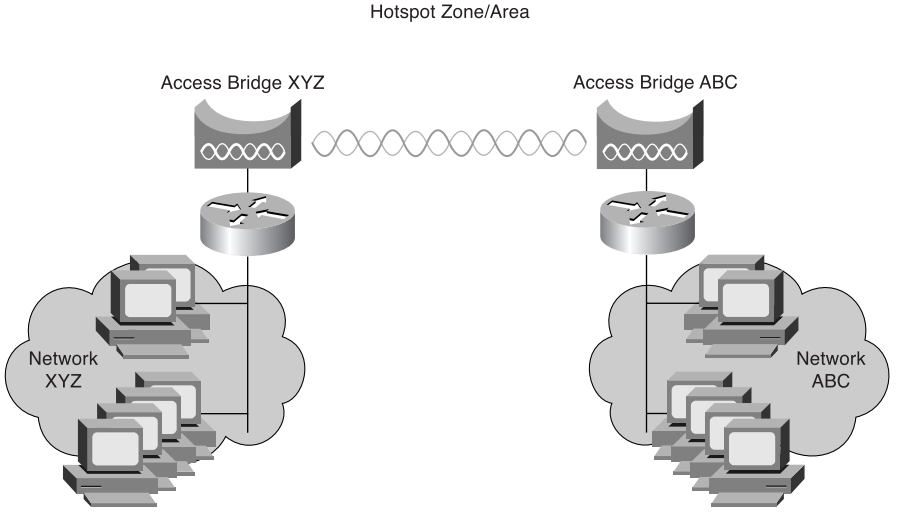
Imagine that Company XYZ acquires Company ABC, which is located in the same business park. The network administrators have the responsibility to establish connectivity between the two companies and integrate Company ABC's infrastructure into Company XYZ's infrastructure. Building-to-building wireless networks might be an option to 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
- Point-to-multipoint

Point-to-point wireless links between buildings can be either radio- or laser-based point-to-point links. Figure 14-3 illustrates the point-to-point wireless setup between two buildings.

Figure 14-3 *Point-to-Point Wireless Network*



Antennas are used to focus the signal power in a narrow beam to maximize the transmission distance. Point-to-point wireless setups can also use laser light as a carrier for data transmission.

Company buildings spread across a campus or business park can also be connected using radio-based point-to-multipoint bridged networks by means of antennas. These antennas use wide beam width to connect multiple buildings.

Cisco provides a family of WLAN products that delivers the same level of security, scalability, and manageability for WLANs that customers have come to expect in their wired LAN. The Cisco Aironet Series offers a complete line of in-building and building-to-building WLAN solutions. The line includes access points, WLAN client adapters, bridges, antennas, and accessories. More information on the Cisco wireless product line can be found at http://www.cisco.com/en/US/products/hw/wireless/index.html.

NOTE More recently, Cisco acquired a company called Linksys, Inc. Linksys, Inc. is a division of Cisco Systems, Inc. and is the leading global manufacturer of broadband, wireless, and networking hardware for home and small office/home office (SOHO) environments. The products are sold under the Linksys brand through its existing retail, distributor, and e-commerce channels.

More information on the Cisco Linksys product line can be found at http://www.linksys.com/Products/.

Linksys has a broad product range, from wireless NICs to access points. Wireless IP cameras, wireless DVD players, and wireless storage devices are some of the latest developments of Linksys.

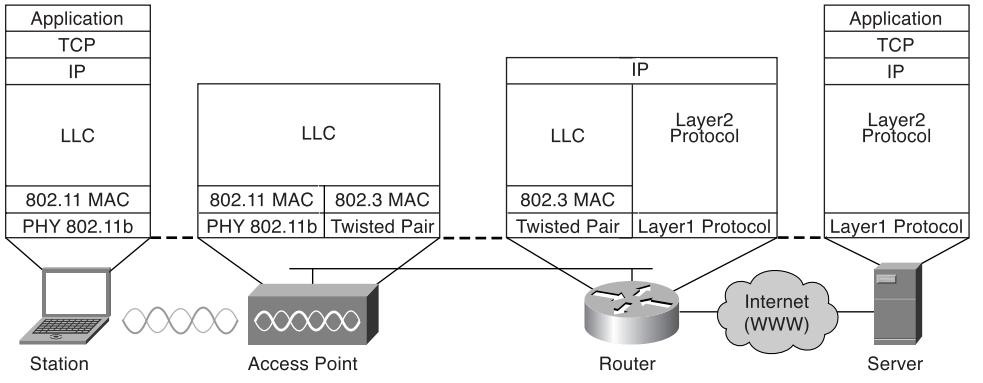
What Is a WLAN?

As stated in the beginning of the chapter, WLANs are networks that are commonly deployed in places such as corporate office conference rooms, industrial warehouses, Internet-ready classrooms, and even coffeehouses. A WLAN uses radio frequency (RF) technology to transmit and receive data over the air, in a manner defined by the predominant standard for wireless IEEE 802.11.

These IEEE 802.11-based WLANs present new challenges for network administrators and information security administrators. Unlike the relative simplicity of wired Ethernet deployments, 802.11-based WLANs broadcast RF data for the client stations to hear.

To understand some of the challenges and weaknesses, an explanation of the protocol stack and the wireless functionality is in order. Figure 14-4 illustrates the 802.11 standard protocol stacks for a client-server application over a wireless network.

Figure 14-4 *802.11 Protocol Stack*



The IEEE 802.11 standard specifies the over-the-air interface between a wireless client and a base station or access point. The standard also specifies the interface for connections among wireless clients. As with any other 802.x standard (802.3 is Ethernet, 802.5 is Token Ring), the 802.11 standard provides specifications to address both the physical (PHY) and medium access control (MAC) layers.

The 802.11 standard was first released in 1997. It specified the MAC sublayer, MAC management protocols and services, and three physical layers providing different data rates. Later releases have improved data rates, security features, and quality of service features. Table 14-1 compares the main differences between the different standards.

Table 14-1 *Overview of 802.11 Standards*

	802.11a	802.11b	802.11g
Frequency	5 GHz	2.4 GHz	2.4 GHz
Rate	54 Mbps	11 Mbps	54 Mbps
Market	Home entertainment	Wireless office	Home and office applications

The data sent according to the 802.11a and 802.11g standards is transmitted at the same rate, but the 5-GHz band has some restrictions and is not as clear as the 2.4-GHz band in some countries. Other 802.11 specifications do exist and are being worked on. This chapter, however, focuses on the 802.11i standard, which is an 802.11 MAC enhancement to provide improved security and authentication mechanisms.

In summary, it is possible to say that, at this moment, the most popular WLAN is the 802.11b used for initial applications in the business world. On the other hand, residential applications

are forecast to explode in the coming years, most likely making 802.11a the de facto wireless standard.

How Wireless Works

The security in the WLAN standard, which applies to 802.11b, 802.11a, and 802.11g, has come under intense scrutiny and inspection. Both researchers and hackers have exposed several vulnerabilities in the authentication, data-privacy, and message-integrity mechanisms defined in the specification. To help you understand these vulnerabilities, the sections that follow go into more detail on how wireless networks work.

WLAN Architecture

WLAN architecture has three components:

- Wireless end stations
- Access points
- Basic service sets

The wireless end station can be any device that can communicate using the 802.11 standard (laptops, workstations, and PDAs, as well as printers and scanners).

The access point (AP) is a device that can provide two functions: It acts as a network platform for connections between WLANs or to a wired LAN and as a relay between stations attached to the same AP.

Whereas the wireless station and the access point are both physical components, the basic service set (BSS) is the logical component of wireless architecture. The BSS in general is a set of wireless stations controlled by a single management function and has two configuration options. In an IBSS, the stations communicate directly to one another without the need for an access point. Please refer to Figure 14-1 to see a configuration in which there is no interconnection to the wired network. In an infrastructure BSS, there is a connection to the wired network. An extended service set (ESS) is a set of infrastructure BSSs that appear as a single BSS. This is important for connection redundancy but has some security issues that need to be addressed.

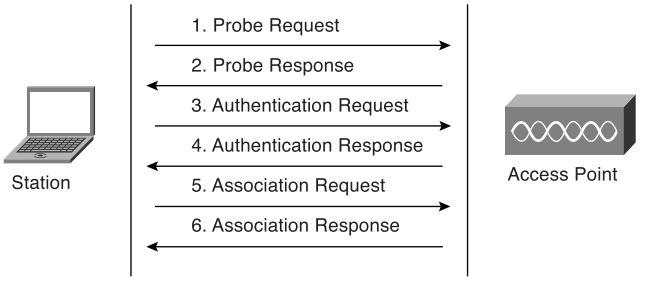
Setting Up the WLAN Connection

Knowing that a WLAN uses RF technology to transmit and receive data over the air, you can easily understand that the first step in the setup process is the scanning function. As with tuning into a radio station, the scanning function needs a wireless station to find other stations or access

points. Therefore, the 802.11 standard defines two different scanning functions, namely active scanning and passive scanning. During the scanning process, the station listens for beacon frames (similar to keepalives) to locate and identify the BSS within the range. The information in the beacon frame contains service set identifiers (SSIDs), supported rates, and timestamps.

Figure 14-5 illustrates the connection setup step by step. Each and every step in the station authentication process is discussed. The 802.11 specification stipulates two mechanisms for authenticating WLAN clients: open authentication and shared key authentication. Two other mechanisms—the SSID and authentication by client MAC address—are also commonly used. The weaknesses of all these mechanisms are addressed in the wireless risk section later in the chapter. Wired equivalent privacy (WEP) keys can function as a type of access control because a client that lacks the correct WEP key cannot send data to or receive data from an access point. WEP, the encryption scheme adopted by the IEEE 802.11 committee, provides encryption with 40 bits or 128 bits of key strength.

Figure 14-5 *Wireless Station Authentication*



NOTE Figure 14-5 is based on content from the following Cisco WLAN white paper: http://www.cisco.com/en/US/netsol/ns339/ns395/ns176/ns178/networking_solutions_white_paper09186a00800b469f.shtml.

As you can see in Figure 14-5, the 802.11 client authentication process consists of six steps:

Step 1 The station broadcasts a probe request frame on every channel, allowing the station to quickly locate either a specific station (via SSID) or any WLAN within range.

Step 2 Access points within range respond with a probe response frame. The response is from the access point in an infrastructure BSS. (For IBSSs, the last station to send a beacon responds.)

Step 3 The client decides which access point (AP) is the best for access and sends an authentication request.

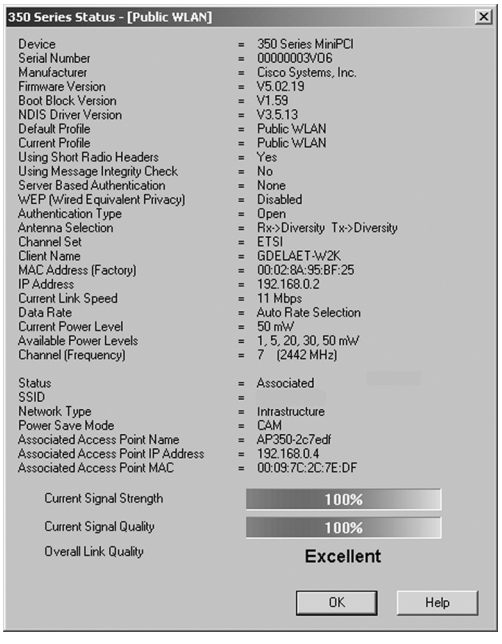
Step 4 The access point sends an authentication reply. This response includes an authentication algorithm ID for open systems. (For shared key systems, WEP is used to generate a random number, and an authentication challenge text is used in the response frame. This results in another request/response encrypted frame pair that is not shown in the figure for simplicity's sake but is discussed later in the chapter.)

Step 5 Upon successful authentication, the client sends an association request frame to the access point. This is an important step to ensure that anyone who wants to send data to the wireless station knows to send data through the access point.

Step 6 The access point replies with an association response.

Figure 14-6 illustrates the station's successful authentication and association with the access point. The client is now able to pass traffic to the access point.

Figure 14-6 *Successful Wireless Station Authentication*



Risks of Open Wireless Ports

As indicated earlier in the chapter, the use of wireless components in the network infrastructure raises big security issues. You want to keep intruders away from accessing your network, reading and modifying network traffic, and so on. In chronological order, the following techniques were developed to resolve these issues: the SSID, Open Authentication protocol, and the WEP protocol. WEP was designed to tackle these issues and provide some level of security on WLANs as on a physical wire.

SSID Vulnerabilities

The SSID is advertised in plain text in the access point beacon messages. Although beacon messages are transparent to users, an eavesdropper can easily determine the SSID with the use of an 802.11 WLAN packet analyzer such as Sniffer Pro, NetStumbler, and Kismet. Some access-point vendors, including Cisco, offer the option of disabling SSID broadcasts in the beacon messages. But this still leaves the option open for an eavesdropper to find out what the SSID is set to by sniffing the probe response frames from an access point. Using only the SSID as a mode of security is not advisable.

Open Authentication Vulnerabilities

Wireless networks with open authentication create major network vulnerabilities. The access point has no means to determine whether a client is valid. For public WLAN deployments, it might not be possible to implement strong authentication; higher-layer authentication might be required.

Shared Key Authentication Vulnerabilities

Before delving into the main vulnerability in WEP, you need to understand the shared key authentication process in more detail.

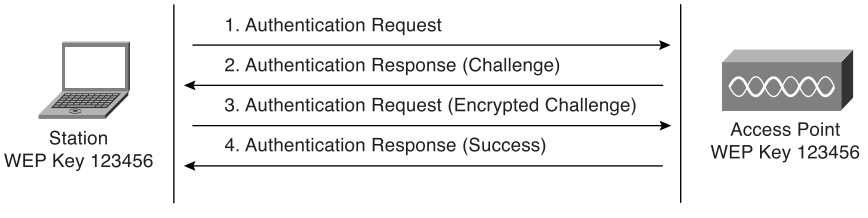
WEP Protocol Overview

The WEP protocol is intended to implement three main security goals:

- Confidentiality
- Access control
- Data integrity

Achieving these goals should help you, as network administrator, prevent unauthorized individuals from using your wireless infrastructure or learning the content of your wireless traffic. The shared key authentication process requires that the client configure a static WEP key. Figure 14-7 describes the shared key authentication process, and the steps that follow describe the steps shown in the figure.

Figure 14-7 *Wireless Station Authentication Using WEP*



Step 1 The client sends an authentication request to the access point requesting shared key authentication.

Step 2 The access point uses the WEP algorithm to generate a random number used in the authentication response containing a challenge text.

Step 3 The client uses its locally configured WEP key to encrypt the challenge text and reply with a subsequent authentication request.

Step 4 If the access point can decrypt the authentication request and retrieve the original challenge text, it responds with an authentication response that grants the client access.

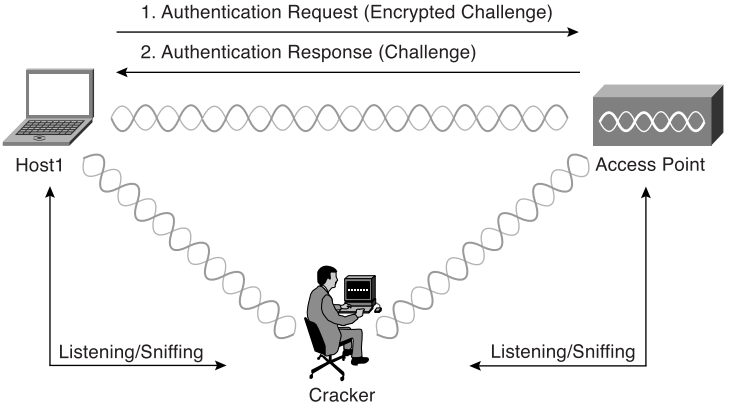
WEP Protocol Vulnerabilities

As you can see in Figure 14-7, the process of exchanging the challenge text occurs over the wireless link and is vulnerable to a man-in-the-middle attack. A cracker can capture both the plain text (challenge text) and the encrypted challenge response.

NOTE For the attack to work, the man-in-the-middle has to decrypt the challenge response to identify the WEP key. Before 2001, programs such as WEPCrack and Airsnort could identify weak WEP keys and challenges, thus making the job of the cracker easy and fast. Vendors have corrected the firmware that creates keys and challenges, so this is no longer the problem that it once was. The phrase "15 minutes to crack WEP via man-in-the-middle attack" was once true but became invalid more than two years ago.

Figure 14-8 illustrates the attack.

Figure 14-8 *WEP Vulnerability*



WEP encryption is done by performing an exclusive OR (XOR) function on the plain text with the key stream to produce the encrypted challenge.

NOTE The XOR function can be stated as, "either A or B, but not both." The XOR function produces logic 1 output only if its two inputs are different. If the inputs are the same, the output is logic 0. This function is often referred to as "add without carry."

It is important to note that if the XOR function is performed on the plain text and on the encrypted challenge, the result is the key stream. Therefore, a cracker can easily derive the key stream just by sniffing the shared key authentication process with a protocol analyzer. Lots of other attacks, such as message modification, message injection, and IP redirection, can be based on the same basic intrusion technique.

It looks as if WEP has not met any of the security goals it was intended to address. As a network administrator, you should assume that WEP is not secure. Treat your wireless network as a public network. Put the wireless network outside your firewall and implement additional authentication methods. Virtual private network (VPN), IP Security (IPSec), and secure shell (SSH) are other pieces of higher layer software that encrypt all data from the client application to the server application to make the transaction secure, even across an unencrypted 802.11 link.

Cisco has recognized the vulnerabilities in 802.11 authentication and data privacy. Therefore, to give network administrators a secure WLAN solution that is scalable and manageable, a proprietary Cisco Wireless Security Suite was developed. This suite of security enhancements augments the wireless LAN security by implementing enhancements to 802.11 authentication and encryption.

Countermeasures to WEP Protocol Vulnerabilities

Now that it is clear that many 802.11 networks employ the standard WEP protocol, which is known to have major faults, some 802.11 vendors have come up with proprietary solutions. Before the official IEEE 802.11i was released, Cisco created proprietary solutions to address WEP protocol vulnerabilities. The WEP protocol contains three components:

- Authentication framework
- Authentication algorithm
- Data privacy or encryption algorithm

The Cisco Wireless Security Suite contains an enhancement that exceeds the WEP functionality for each of the components in the previous list.

The IEEE 802.1x standard provides a framework for authentication. A new user-based authentication algorithm with the ability to generate dynamic WEP keys has been developed. This algorithm is called the Extensible Authentication Protocol (EAP). Cisco Light Extensible

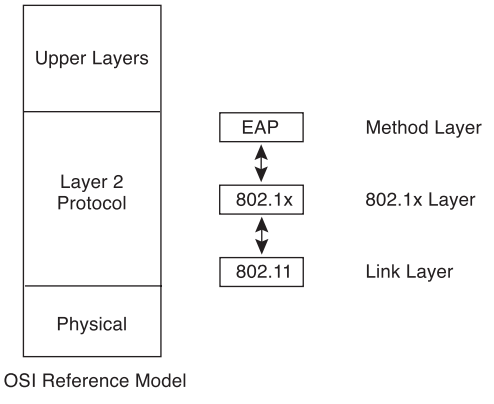
Authentication Protocol (LEAP) is a proprietary Cisco authentication protocol designed for use in IEEE 802.11 WLAN environments. LEAP's main focuses are on mutual authentication between the network infrastructure and the user, secure derivation of random and user-specific cryptographic session keys, and most importantly, compatibility with existing and widespread network authentication mechanisms (for example, RADIUS).

Additionally, Cisco has developed the Temporal Key Integration Protocol (TKIP) to improve WEP privacy and encryption.

EAP Protocol and the 802.11i Standard

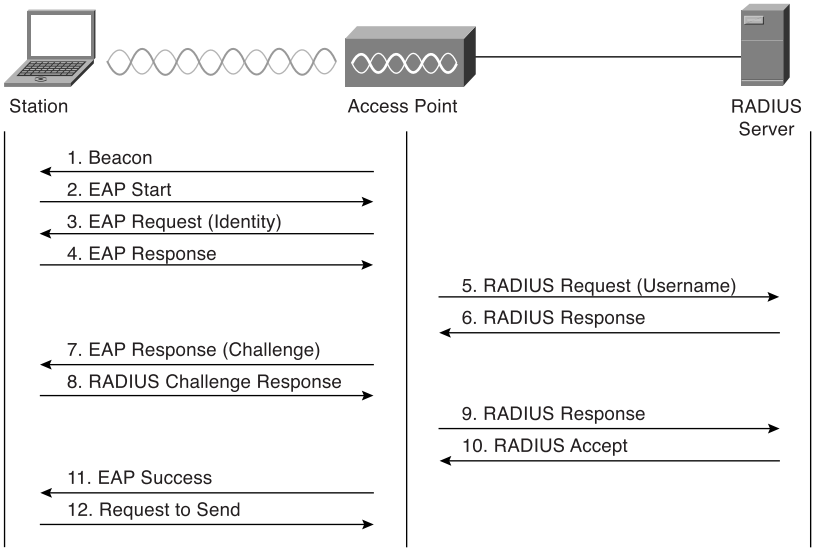
The 802.1x authentication framework is included in the draft for 802.11 MAC layer security enhancements in the IEEE 802.11i specification. The 802.1x framework provides the link layer with extensible authentication normally seen in higher layers. One of the higher layers is EAP, which is also Cisco proprietary. EAP allows negotiation of an authentication protocol for authenticating its peer before allowing network layer protocols to transmit over the link. Figure 14-9 illustrates the relationship between these sublayers.

Figure 14-9 *802.1x Authentication Framework*



EAP is defined in RFC 2284 and was developed to provide strong, easy-to-deploy, and easy-to-administer wireless security. Cisco offers third-party NIC support and RADIUS support to allow customers to use their existing investments in wireless clients as well as existing RADIUS servers. Figure 14-10 illustrates the message flow for the EAP protocol with RADIUS as the authentication method.

Figure 14-10 *Authentication Framework with RADIUS*



As you can see in Figure 14-10, the authentication framework process consists of multiple steps:

Step 1 The station determines 802.11i support from a beacon that is transmitted from the access point.

Step 2 The station starts the session with an EAP frame.

Step 3 The access point sends an EAP identity request message back to the station.

Step 4 The station sends an EAP response (including the station's ID).

Step 5 The access point forwards the packet to the RADIUS server.

Step 6 The RADIUS server sends a response back to the access point including a challenge (EAP authentication type).

Step 7 The access point forwards the challenge to the station.

Step 8 The station sends a challenge response message back (EAP type set to RADIUS).

Step 9 The access point forwards the response to the RADIUS server.

Step 10 The RADIUS server sends an accept message to the access point.

Step 11 The access point forwards an EAP success message to the station.

Step 12 The station is ready to send data.

At this point in time, VPN, IPSec, and SSH, which encrypt all data from the client applications to server applications, make the transaction more secure than only EAP. They are therefore recommended as an additional implemented security layer.

Network administrators should be aware that WLAN deployments should be made as secure as possible, knowing that security is weak in the 802.11 standard. Adding the Cisco Wireless Security Suite can increment security and help to create secure WLANs. The following link describes the Cisco Wireless Security Suite: http://www.cisco.com/en/US/netsol/ns340/ns394/ns348/ns386/networking_solutions_white_paper09186a00800b3d27.shtml.

War-Driving and War-Chalking

War-driving can be best described as a new form of hacking into the network. Crackers are equipped with an antenna either inside their cars or on the roof of their cars. The antenna is connected to a laptop in the car. Once installed in the car, the crackers start driving (or sometimes just park in garages) and log data as they go. Special software logs the latitude and longitude of the car's position as well as the signal strength and network name.

It is important to be aware that companies are opening back doors in their systems to a new type of network intrusion. It is vital for companies to use security network auditing on the wireless section of their networks. No matter how many firewalls are installed in the network, inappropriate wireless configurations can give the cracker access to the corporate network without having to pass through a single firewall.

The term "war-chalking" was inspired by the use of chalk marks in old wartime days. During the 1930s and 1940s, homeless, wandering men used chalk marks to advise their colleagues of places that offered free food or places to wash up. Today, war-chalking is actually creating a language for indicating free Internet access. It can be best described as marking a series of well-defined symbols on sidewalks, walls, pillars, and others structures to indicate nearby wireless access. Each symbol defines a specific wireless setting. This practice enables users to go to those marked locations and use the symbols to figure out what the settings are to connect through a wireless connection to the Internet.

SAFE WLAN Design Techniques and Considerations

The SAFE WLAN design is part of the overall SAFE design guide, which was briefly discussed in Chapter 6, "Secure Design." The SAFE blueprint from Cisco for network security offers a defense-in-depth, modular approach to security that can evolve and change to meet the needs of businesses.

This section of the chapter integrates the previously discussed weaknesses with mitigation techniques, which are then applied to a variety of different networks. The size and security concerns of a specific design dictate the mitigation techniques that are applied to a WLAN design.

For instance, in 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. The designs are based on the assumption that most services available to the wired network are also available to the wireless network addition. All designs include the following WLAN security recommendations. The list differentiates between recommendations for access points and stations.

NOTE The following list is just an example. For a complete list, please refer to the document "Cisco SAFE: WLAN Security in Depth," which covers the standard WLAN design guidelines. You can find the document at the following website: http://www.cisco.com/en/US/netsol/ns340/ns394/ns171/ns128/networking_solutions_white_paper09186a008009c8b3.shtml.

Access point recommendations:

- Enable centralized user authentication (RADIUS, TACACS+) for the management interface.
- Consider using Simple Network Management Protocol (SNMP) Read Only if your management infrastructure allows it.
- Enable wireless frame encryption where available.
- Physically secure the access point.

Station recommendations:

- Enable wireless frame encryption where available.
- Use password protection for all your wireless devices.

NOTE More information on the SAFE WLAN design guide can be found at

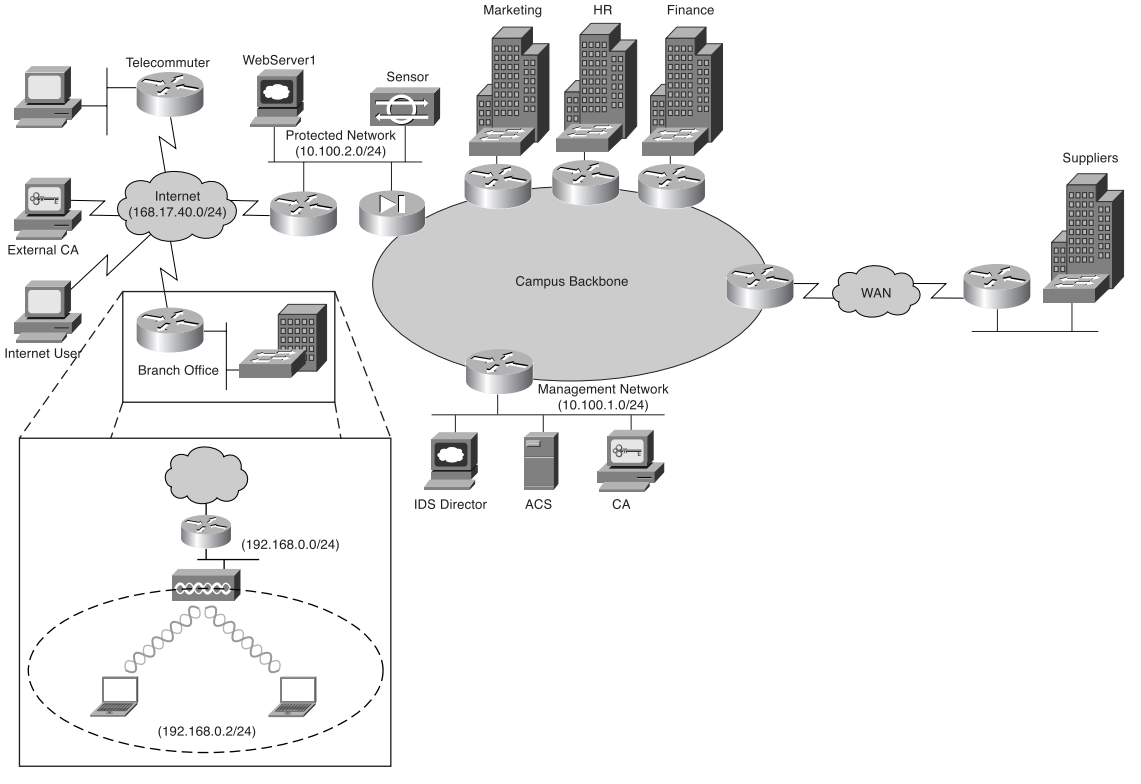
http://www.cisco.com/en/US/netsol/ns340/ns394/ns171/ns128/networking_solutions_white_paper09186a008009c8b3.shtml.

In this document, the reader can notice that distinctions are made for the following types of WLAN design: large network, medium network, small network, and remote user.

Case Study: Adding Wireless Solutions to a Secure Network

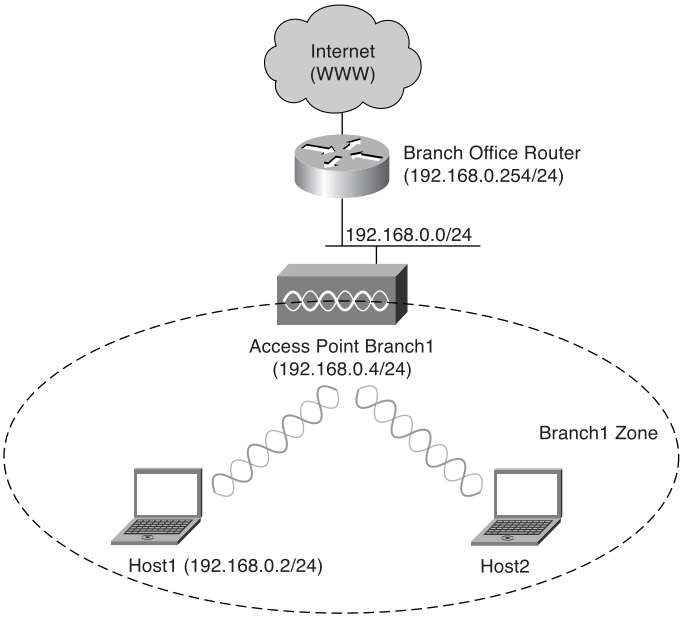
This case study covers the placement and configuration of a wireless access point in a real scenario. The setup and configuration of the wireless stations are covered, and there are screenshots of both the access point and the station. Figure 14-11 illustrates the Company XYZ network diagram for this scenario.

Figure 14-11 *Company XYZ Top-Level Network Layout*



The CIO of Company XYZ has decided to integrate wireless technology throughout the company. The IT department has started the testing and planning phase and wants to roll out a pilot in a branch office of the company. Figure 14-12 zooms in on Figure 14-11 so only the relevant devices for this case study are shown.

Figure 14-12 *Company XYZ—Branch Office Setup*



A local IT engineer starts to configure the access point according to the WLAN design specs defined in the company's security policy.

Figure 14-13 features a sample screenshot of the basic configuration of the access point.

Figure 14-13 *Branch Office Access Point—Basic Setup*

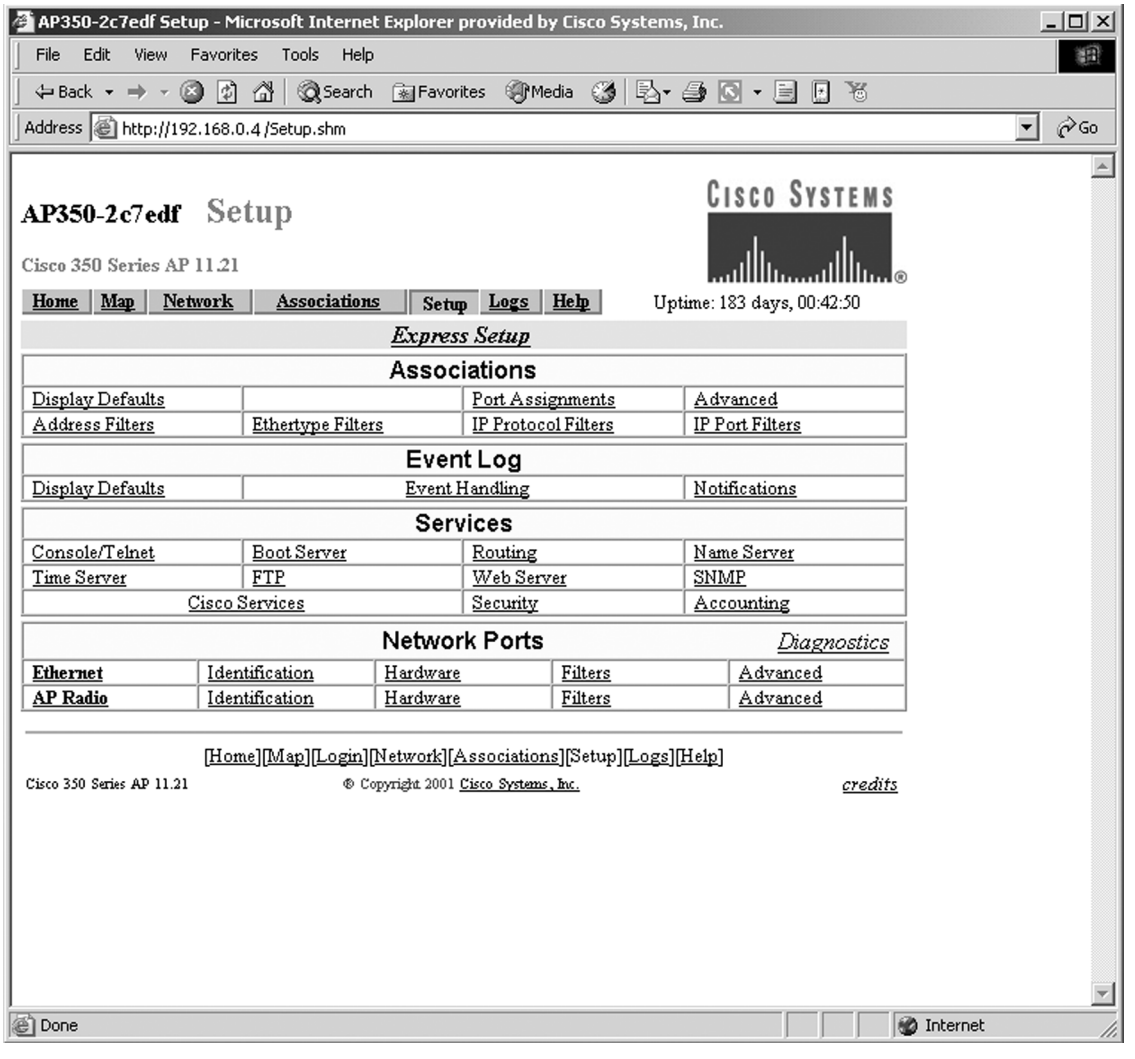


Table 14-2 displays the main parameters of the express setup page used during the initial setup of the access point.

Table 14-2 *Basic Access Point Options*

Syntax	Description
System Name	Identifies the access point on your network
Configuration Server Protocol	Used to match the method of IP address assignment
Default IP Address	Assigns the access point's IP address
Default IP Subnet Mask	Assigns the access point's IP subnet mask
Default IP Gateway	Assigns the access point's IP gateway
Radio Service Set ID (SSID)	Is a unique identifier that client devices use to associate with the access point
SNMP Admin. Community	Enables SNMP through the entry of a string

Now that the access point is set up, the client (Host 1-192.168.0.2) can be configured using the wireless client software. During the setup, a corresponding SSID of the access point was entered. Figure 14-14 illustrates the main page of the client software utility.

Figure 14-14 *Wireless Client Utility*

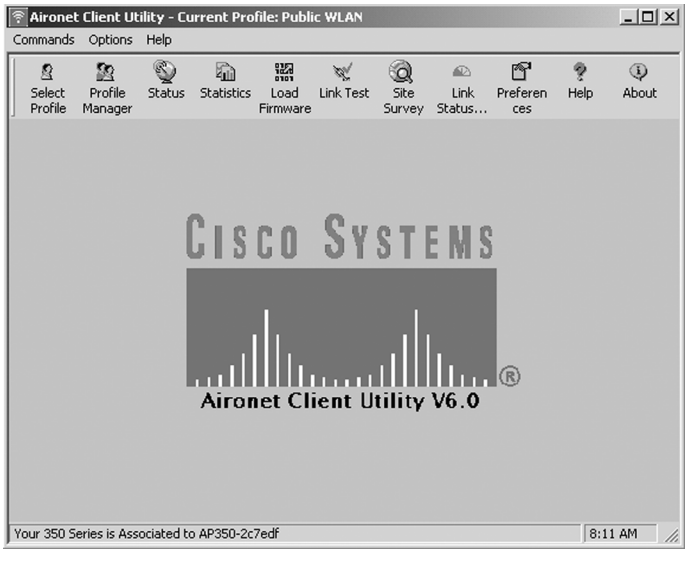
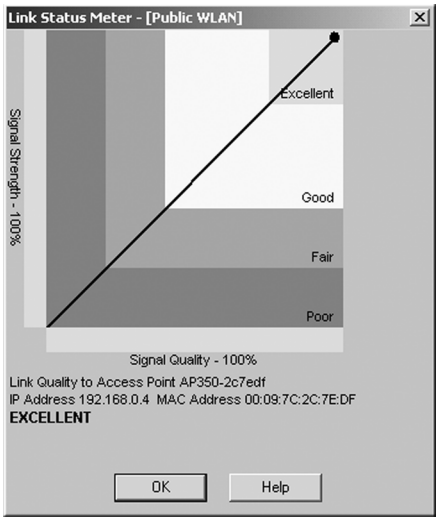


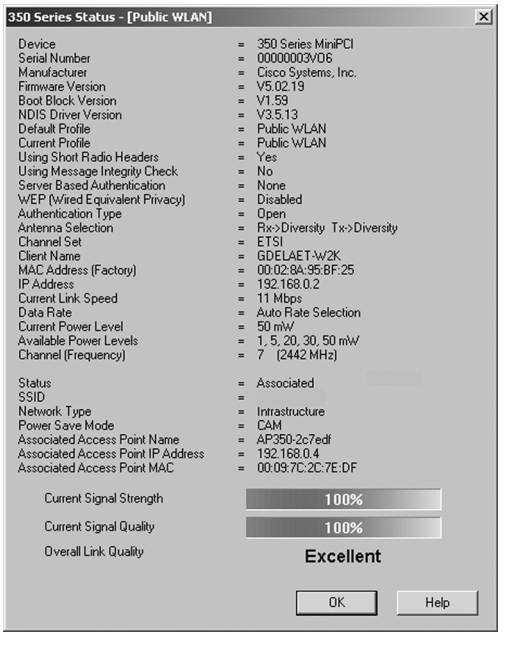
Figure 14-15 shows the link status meter.

Figure 14-15 *Wireless Link Status*



At the bottom of the screen shown in Figure 14-15, notice that the signal strength and signal quality are excellent. Furthermore, Host 1 is associated with access point 192.168.0.4, which is the branch office access point. Figure 14-16 gives the overall status of the wireless connection.

Figure 14-16 *Wireless Status*



The wireless case study covered the placement and configuration of a wireless access point and one sample client setup for Company XYZ. The case study illustrated that the implementation of wireless equipment in a network is fairly easy.

Conclusion

When implementing wireless technologies in a secure network, some points need to be taken into consideration. Some risks are involved in offering wireless connections in your company. This chapter covered the different WLAN configurations and how WLANs work. The SAFE WLAN design techniques can be used to counter the risks of open wireless ports.

Q&A

1. List three categories of WLANs.
2. Which IEEE standards define WLANs?
   - **a** IEEE 802.3
   - **b** IEEE 802.5
   - **c** IEEE 802.11
   - **d** IEEE 802.10
3. The IEEE 802.11 standard specifies the over-the-air interface between what two entities?
4. What are the correct parameters for the 802.11b standard?
   - **a** 2.4 GHz, 11 Mbps, and wireless office
   - **b** 5 GHz, 11 Mbps, and wireless office
   - **c** 2.4 GHz, 54 Mbps, and wireless office
   - **d** 5 GHz, 54 Mbps, and wireless office
5. What are the correct parameters for the 802.11a standard?
   - **a** 2.4 GHz, 11 Mbps, and wireless office
   - **b** 5 GHz, 54 Mbps, and wireless office
   - **c** 2.4 GHz, 54 Mbps, and wireless office
   - **d** 5 GHz, 54 Mbps, and home entertainment

6 What does the acronym SSID stand for?

7 List the three main security goals of the WEP protocol.

8 List the three components of the WEP protocol.

9 What is war-chalking?

10 Security weaknesses in the IEEE 802.11 standard are addressed in which of the following?

- **a** IEEE 802.11a
- **b** IEEE 802.11b
- **c** IEEE 802.11j
- **d** IEEE 802.11i