CHAPTER 3

Wireless LANs

Historically, LANs have been limited to physical wired segments. With the advent of technologies that utilize infrared (IR) and radio frequency (RF) to carry data, LANs are free from the limitations of a physical media. This chapter describes the reasons for extending the reach of a LAN and the methods that can be used to do so, with a focus on RF wireless access.

Chapter Objectives

Upon completing this chapter, you will be able to describe the wireless LAN (WLAN) environment. This includes being able to meet the following objectives:

- Describe the business drivers and standards that affect WLAN implementation
- Describe WLAN security issues and threat-mitigation methods
- Describe the factors that affect WLAN implementation

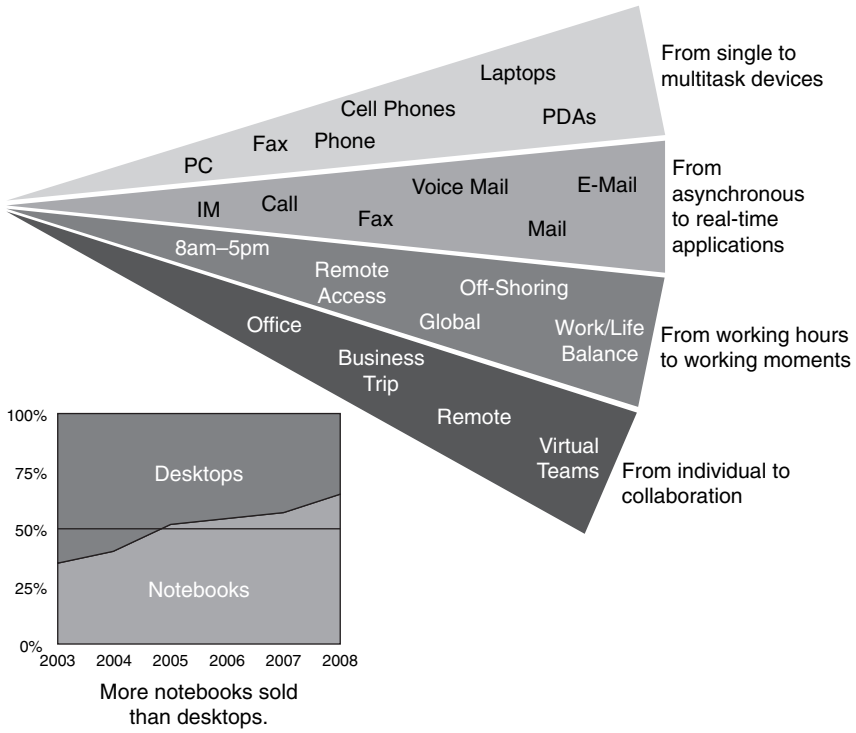
Exploring Wireless Networking

Wireless networking technology has developed like most new technologies; business needs drive technology developments, which in turn drive new business needs, which in turn drive new technology developments. To keep this cycle from spinning out of control, several organizations have stepped forward to establish WLAN standards and certifications. This lesson describes the trends and standards that impact WLAN development.

The Business Case for WLAN Service

Productivity is no longer restricted to a fixed work location or a defined time period. People now expect to be connected at any time and place, from the office to the airport or even the home. Traveling employees used to be restricted to pay phones for checking messages and returning a few phone calls between flights. Now employees can check e-mail, voice mail, and the web status of products on personal digital assistants (PDA) while walking to a flight. Figure 3-1 shows the trends involved with wireless networking and mobility.

Figure 3-1 *Wireless Market Trends*



Even at home, people have changed the way they live and learn. The Internet has become a standard in homes, right along with TV and phone service. Even the method of accessing the Internet has quickly moved from temporary modem dialup service to dedicated digital subscriber line (DSL) or cable service, which is always connected and is faster than dialup. In 2005, users of PCs purchased more Wi-Fi–enabled mobile laptops (i.e., products that are based on the IEEE 802.11 standards) than fixed-location desktops.

The most tangible benefit of wireless is the cost reduction. Two situations illustrate cost savings. First, with a wireless infrastructure already in place, savings are realized when moving a person from one location in an office to another, when reorganizing a lab, or when moving from temporary locations or project sites. On average, the IT cost of moving an employee from one location to another where wiring changes are required is $375. For the business case, assume that 15 percent of the staff is moved every year. With a staff of 800, the savings represented by using wireless would be $45,000. The second situation to consider is when a company moves into a new building that does not have a wired infrastructure. In this case, the savings from wireless is even more noticeable because running cables through walls, ceilings, and floors is a labor-intensive process.

Finally, another advantage of using a WLAN is the increase in employee satisfaction brought on by having mobility in their working environment, leading to less turnover and the cost savings of not hiring as many new employees. Employee satisfaction also results in better customer support, which can't be easily quantified, but is a major benefit.

Besides the increase in productivity, WLAN also means better quality in daily work (better responsiveness to customers, a better can-do attitude from employees, and so on) and other benefits that cannot be easily measured.

Differences Between WLANs and LANs

Although WLANs and LANs both provide connectivity between the end users, they have some key differences that include both physical and logical differences between the topologies. In WLANs, radio frequencies are used as the physical layer of the network. Differences also exist in the way the frame is formatted and in the transmission methods, detailed as follows:

- WLANs use carrier sense multiple access with collision avoidance (CSMA/CA) instead of carrier sense multiple access collision detect (CSMA/CD), which is used by Ethernet LANs. Collision detection is not possible in WLANs, because a sending station cannot receive at the same time that it transmits and, therefore, cannot detect a collision. Instead, WLANs use the Ready To Send (RTS) and Clear To Send (CTS) protocols to avoid collisions.
- WLANs use a different frame format than wired Ethernet LANs use. WLANs require additional information in the Layer 2 header of the frame.

Radio waves cause problems not found in LANs, such as the following:

- Connectivity issues occur because of coverage problems, RF transmission, multipath distortion, and interference from other wireless services or other WLANs.
- Privacy issues occur because radio frequencies can reach outside the facility.

In WLANs, mobile clients connect to the network through an access point, which is the equivalent of a wired Ethernet hub. These connections are characterized as follows:

- There is no physical connection to the network.
- The mobile devices are often battery-powered, as opposed to plugged-in LAN devices.

WLANs must meet country-specific RF regulations. The aim of standardization is to make WLANs available worldwide. Because WLANs use radio frequencies, they must follow country-specific regulations of RF power and frequencies. This requirement does not apply to wired LANs.

Radio Frequency Transmission

Radio frequencies range from the AM radio band to frequencies used by cell phones. This section identifies the characteristics of the radio frequency transmissions used by WLANs.

Radio frequencies are radiated into the air by antennas that create radio waves. When radio waves are propagated through objects, they might be absorbed, scattered, or reflected. This absorption, scattering, and reflection can cause areas of low signal strength or low signal quality. Understanding this phenomena and the causes is important when you are building and designing WLAN networks.

The transmission of radio waves is influenced by the following factors:

- **Reflection:** Occurs when RF waves bounce off objects (for example, metal or glass surfaces)
- **Scattering:** Occurs when RF waves strike an uneven surface (for example, a rough surface) and are reflected in many directions
- **Absorption:** Occurs when RF waves are absorbed by objects (for example, walls)

The following rules apply for data transmission over radio waves:

- Higher data rates have a shorter range because the receiver requires a stronger signal with a better signal-to-noise ratio (SNR) to retrieve the information.
- Higher transmit power results in a greater range. To double the range, the power has to be increased by a factor of four.
- Higher data rates require more bandwidth. Increased bandwidth is possible with higher frequencies or more complex modulation.
- Higher frequencies have a shorter transmission range because they have higher degradation and absorption. This problem can be addressed by more efficient antennas.

Organizations That Standardize WLANs

Several organizations have stepped forward to establish WLAN standards and certifications. This topic identifies the organizations that define WLAN standards.

Regulatory agencies control the use of the RF bands. With the opening of the 900-MHz Industrial, Scientific, and Medical (ISM) band in 1985, the development of WLANs started. New transmissions, modulations, and frequencies must be approved by regulatory agencies. A worldwide consensus is required. Regulatory agencies include the Federal

Communications Commission (FCC) for the United States (http://www.fcc.gov) and the European Telecommunications Standards Institute (ETSI) for Europe (http://www.etsi.org).

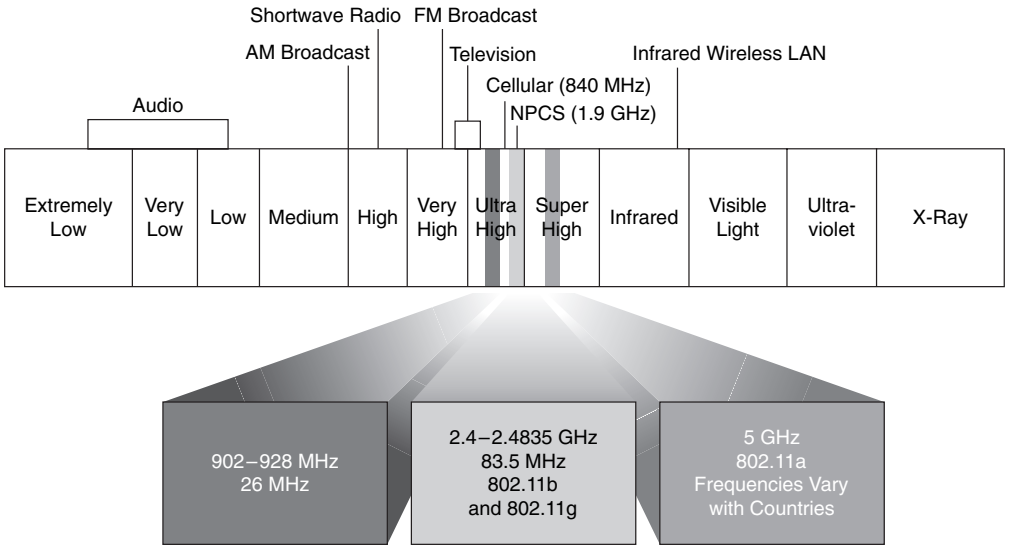
The Institute of Electrical and Electronic Engineers (IEEE) defines standards. IEEE 802.11 is part of the 802 networking standardization process. You can download ratified standards from the IEEE website (http://standards.ieee.org/getieee802).

The Wi-Fi Alliance offers certification for interoperability between vendors of 802.11 products. Certification provides a comfort zone for purchasers of these products. It also helps market WLAN technology by promoting interoperability between vendors. Certification includes all three 802.11 RF technologies and Wi-Fi Protected Access (WPA), a security model released in 2003 and ratified in 2004, based on the new security standard IEEE 802.11i, which was ratified in 2004. The Wi-Fi Alliance promotes and influences WLAN standards. A list of ratified products can be found on the Wi-Fi website (http://www.wi-fi.org).

ITU-R Local FCC Wireless

Several unlicensed RF bands exist. Figure 3-2 shows an overview of the FCC bands and where the wireless bands are located.

Figure 3-2 *Wireless Bands*



Three unlicensed bands exist: 900 MHz, 2.4 GHz, and 5.7 GHz. The 900-MHz and 2.4-GHz bands are referred to as the ISM bands, and the 5-GHz band is commonly referred to as the Unlicensed National Information Infrastructure (UNII) band.

Frequencies for these bands are as follows:

- **900-MHz band:** 902 MHz to 928 MHz.
- **2.4-GHz band**: 2.400 GHz to 2.483 GHz (in Japan, this band extends to 2.495 GHz.)
- **5-GHz band:** 5.150 GHz to 5.350 GHz, 5.725 GHz to 5.825 GHz, with some countries supporting middle bands between 5.350 GHz and 5.725 GHz. Not all countries permit IEEE 802.11a, and the available spectrum varies widely. The list of countries that permit 802.11a is changing.

Figure 3-2 shows WLAN frequencies. Next to the WLAN frequencies in the spectrum are other wireless services such as cellular phones and Narrowband Personal Communication Services (NPCS). The frequencies used for WLAN are ISM bands.

A license is not required to operate wireless equipment on unlicensed frequency bands. However, no user has exclusive use of any frequency. For example, the 2.4-GHz band is used for WLANs, video transmitters, Bluetooth, microwave ovens, and portable phones. Unlicensed frequency bands offer best-effort use, and interference and degradation are possible.

Even though these frequency bands do not require a license to operate equipment, they still are subject to the local country's code regulations inside the frequencies to regulate areas such as transmitter power, antenna gain (which increases the effective power), and the sum of transmitter loss, cable loss, and antenna gain.

Effective Isotropic Radiated Power (EIRP) is the final unit of measurement monitored by local regulatory agencies. Therefore, caution should be used when attempting to replace a component of a WLAN, for example, when adding or upgrading an antenna to increase range. The possible result could be a WLAN that is illegal under local codes. The equation for calculating EIRP is as follows:

EIRP = transmitter power + antenna gain – cable loss

NOTE Use only antennas and cables supplied by the original manufacturer listed for the specific access point implementation. Use only qualified technicians who understand the many different requirements of the country's RF regulatory codes.

802.11 Standards Comparison

IEEE standards define the physical layer and the Media Access Control (MAC) sublayer of the data link layer of the OSI model. The original 802.11 wireless standard was completed in June, 1997. It was revised in 1999 to create IEEE 802.11a/b and then reaffirmed in 2003 as IEEE 802.11g.

By design, the standard does not address the upper layers of the OSI model. IEEE 802.11b was defined using Direct Sequence Spread Spectrum (DSSS). DSSS uses just one channel that spreads the data across all frequencies defined by that channel. Table 3-1 shows the different standards and how they compare.

Table 3-1 *802.11 Standards*

Standard	802.11b	802.11a	802.11g	
Frequency band	2.4 GHz	5 GHz	2.4 GHz	
Number of channels	3	Up to 23	3	
Transmission	Direct Sequence Spread Spectrum (DSSS)	Orthogonal Frequency Division Multiplexing (OFDM)	Direct Sequence Spread Spectrum (DSSS)	Orthogonal Frequency Division Multiplexing (OFDM)
Data Rates in Mbps	1, 2, 5.5, 11	6, 9, 12, 18, 24, 36, 48, 54	1, 2, 5.5, 11	6, 9, 12, 18, 24, 36, 48, 54

IEEE 802.11 divided the 2.4-GHz ISM band into 14 channels, but local regulatory agencies such as the FCC designate which channels are allowed, such as channels 1 through 11 in the United States. Each channel in the 2.4 GHz ISM band is 22 MHz wide with 5 MHz separation, resulting in overlap with channels before or after a defined channel. Therefore, a separation of 5 channels is needed to ensure unique nonoverlapping channels. Given the FCC example of 11 channels, the maximum of nonoverlapping frequencies are channels 1, 6, and 11.

Recall that wireless uses half-duplex communication, so the basic throughput is only about half of the data rate. Because of this, the IEEE 802.11b main development goal is to achieve higher data rates within the 2.4-GHz ISM band to continue to increase the Wi-Fi consumer market and encourage consumer acceptance of Wi-Fi.

802.11b defined the usage of DSSS with newer encoding or modulation of Complementary Code Keying (CCK) for higher data rates of 5.5 and 11 Mbps (Barker Coding of 1 and 2 Mbps). 802.11b still uses the same 2.4-GHz ISM band and is backward compatible with prior 802.11 and its associated data rates of 1 and 2 Mbps.

The year that the 802.11b standard was adopted, IEEE developed another standard known as 802.11a. This standard was motivated by the goal of increasing data rates by using a different OFDM spread spectrum and modulation technology and using the less crowded frequency of 5 GHz UNII. The 2.4-GHz ISM band was widely used for all WLAN devices, such as Bluetooth, cordless phones, monitors, video, and home gaming consoles, and it also happens to be the same frequency used by microwave ovens. 802.11a was not as widely known because materials for chip manufacturing were less readily available and initially resulted in higher cost. Most applications satisfied the requirements following the cheaper and more accessible standards of 802.11b.

A more recent development by IEEE maintains usage of the 802.11 MAC and obtains higher data rates in the 2.4-GHz ISM band. The IEEE 802.11g amendment uses the newer OFDM from 802.11a for higher speeds, yet is backward compatible with 802.11b using DSSS, which was already using the same ISM frequency band. DSSS data rates of 1, 2, 5.5, and 11 Mbps are supported, as are OFDM data rates of 6, 9, 12, 18, 24, 48, and 54 Mbps. IEEE requires only mandatory data rates of OFDM using 6, 12, and 24 Mbps, regardless whether it is 802.11a or 802.11g OFDM.

Wi-Fi Certification

Even after the 802.11 standards were established, a need to ensure interoperability among 802.11 products still existed. The Wi-Fi Alliance is a global, nonprofit industry trade association devoted to promoting the growth and acceptance of wireless LANs. One of the primary benefits of the Wi-Fi Alliance is to ensure interoperability among 802.11 products offered by various vendors by providing certification. Figure 3-3 shows an example of the Wi-Fi Alliance certification logo.

Figure 3-3 *Wi-Fi Alliance Certification Logo*

Certified vendor interoperability provides a comfort zone for purchasers. Certification includes all three IEEE 802.11 RF technologies, as well as an early adoption of pending IEEE drafts, such as one that addresses security. The Wi-Fi Alliance adapted the IEEE 802.11i draft security as WPA and then revised it to WPA2 after final release of IEEE 802.11i.

Summary of Exploring Wireless Networking

The following summarizes the key points that were discussed in this section:

- People now expect to be connected at any time at any place. However, the most tangible benefit of wireless is cost reduction.
- Both WLANs and LANS use CSMA. However, WLANs use CA, whereas LANs used CD.
- Radio frequencies are radiated into the air by antennas where they are affected by:
  - Reflection
  - Scattering
  - Absorption
- The IEEE defines the 802.11 standards.
- The ITU-R local FCC wireless bands are unlicensed.
- The 802.11 standards are a set of standards that define the frequencies and radio bands for WLANs.
- One of the primary benefits of the Wi-Fi Alliance is to ensure interoperability among 802.11 products.

Understanding WLAN Security

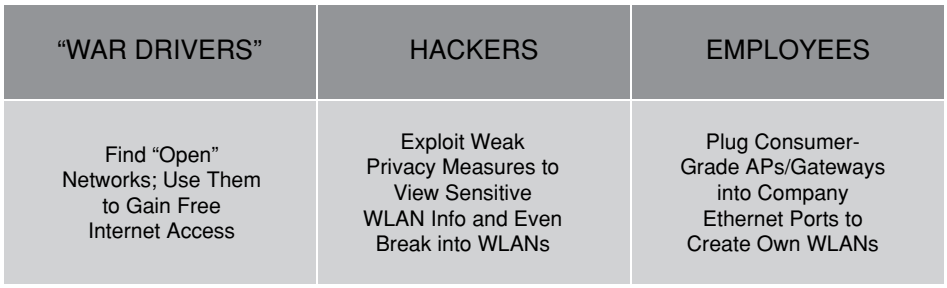
As discussed previously, the most tangible benefit of wireless is cost reduction. In addition to increasing productivity, WLANs increase work quality. However, a security breach resulting from a single unsecured access point can negate hours spent securing the corporate network and even ruin an organization. You must understand the security risks of WLANs and how to reduce those risks.

After completing this section, you will be able to describe WLAN security issues and the features available to increase WLAN security.

Wireless LAN Security Threats

With the lower costs of IEEE 802.11b/g systems, it is inevitable that hackers have many more unsecured WLANs from which to choose. Incidents have been reported of people using numerous open source applications to collect and exploit vulnerabilities in the IEEE 802.11 standard security mechanism, Wired Equivalent Privacy (WEP). Wireless sniffers enable network engineers to passively capture data packets so that they can be examined to correct system problems. These same sniffers can be used by hackers to exploit known security weaknesses. Figure 3-4 shows the most common threats to wireless networks.

Figure 3-4 *Wireless LAN Threats*



"War driving" originally meant using a cellular scanning device to find cell phone numbers to exploit. War driving now also means driving around with a laptop and an 802.11b/g client card to find an 802.11b/g system to exploit.

Most wireless devices sold today are WLAN-ready. End users often do not change default settings, or they implement only standard WEP security, which is not optimal for securing wireless networks. With basic WEP encryption enabled (or, obviously, with no encryption enabled), collecting data and obtaining sensitive network information, such as user login information, account numbers, and personal records, is possible.

A rogue access point (AP) is an AP placed on a WLAN and used to interfere with normal network operations, for example, with denial of service (DoS) attacks. If a rogue AP is programmed with the correct WEP key, client data could be captured. A rogue AP also could be configured to provide unauthorized users with information such as MAC addresses of clients (both wireless and wired), to capture and spoof data packets, or, at worst, to gain access to servers and files. A simple and common version of a rogue AP is one installed by employees with authorization. Employees install access points intended for home use without the necessary security configuration on the enterprise network, causing a security risk for the network.

Mitigating Security Threats

To secure a WLAN, the following components are required:

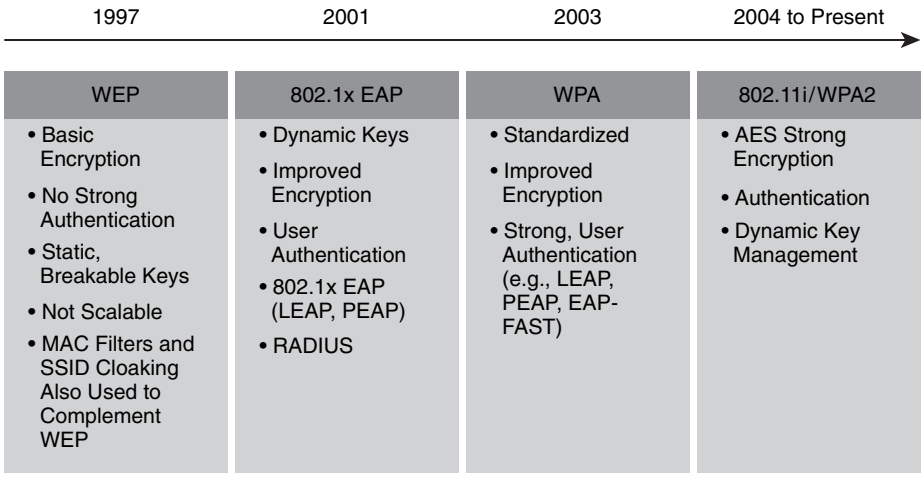
- **Authentication:** To ensure that legitimate clients and users access the network via trusted access points
- **Encryption:** To provide privacy and confidentiality
- **Intrusion Detection Systems (IDS) and Intrusion Protection Systems (IPS):** To protect from security risks and availability

The fundamental solution for wireless security is authentication and encryption to protect the wireless data transmission. These two wireless security solutions can be implemented in degrees; however, both apply to small office/home office (SOHO) and large enterprise wireless networks. Larger enterprise networks need the additional levels of security offered by an IPS monitor. Current IPS systems do not only detect wireless network attacks, but also provide basic protection against unauthorized clients and access points. Many enterprise networks use IPS for protection not primarily against outside threats, but mainly against unintentional unsecured access points installed by employees desiring the mobility and benefits of wireless.

Evolution of Wireless LAN Security

Almost as soon as the first WLAN standards were established, hackers began trying to exploit weaknesses. To counter this threat, WLAN standards evolved to provide more security. Figure 3-5 shows the evolution of WLAN security.

Figure 3-5 *Evolution of Wireless LAN Security*



Initially, 802.11 security defined only 64-bit static WEP keys for both encryption and authentication. The 64-bit key contained the actual 40-bit key plus a 24-bit initialization vector. The authentication method was not strong, and the keys were eventually compromised. Because the keys were administered statically, this method of security was not scalable to large enterprise environments. Companies tried to counteract this weakness with techniques such as Service Set Identifier (SSID) and MAC address filtering.

The SSID is a network-naming scheme and configurable parameter that both the client and the AP must share. If the access point is configured to broadcast its SSID, the client associates with the access point using the SSID advertised by the access point. An access

point can be configured to not broadcast the SSID (SSID cloaking) to provide a first level of security. The belief is that if the access point does not advertise itself, it is harder for hackers to find it. To allow the client to learn the access point SSID, 802.11 allows wireless clients to use a null string (no value entered in the SSID field), thereby requesting that the access point broadcast its SSID. However, this technique renders the security effort ineffective because hackers need only send a null string until they find an access point.

Access points also support filtering using a MAC address. Tables are manually constructed on the AP to allow or disallow clients based upon their physical hardware address. However, MAC addresses are easily spoofed, and MAC address filtering is not considered a security feature.

While 802.11 committees began the process of upgrading WLAN security, enterprise customers needed wireless security immediately to enable deployment. Driven by customer demand, Cisco introduced early proprietary enhancements to RC4-based WEP encryption. Cisco implemented Temporal Key Integrity Protocol (TKIP) per-packet keying or hashing and Cisco Message Integrity Check (Cisco MIC) to protect WEP keys. Cisco also adapted 802.1x wired authentication protocols to wireless and dynamic keys using Cisco Lightweight Extensible Authentication Protocol (Cisco LEAP) to a centralized database.

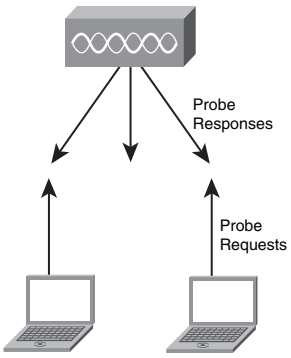
Soon after the Cisco wireless security implementation, the Wi-Fi Alliance introduced WPA as an interim solution that was a subset of the expected IEEE 802.11i security standard for WLANs using 802.1x authentication and improvements to WEP encryption. The newer key-hashing TKIP versus Cisco Key Integrity Protocol and message integrity check (MIC versus Cisco MIC) had similar features but were not compatible.

Today, 802.11i has been ratified, and Advanced Encryption Standard (AES) has replaced WEP as the latest and most secure method of encrypting data. Wireless Intrusion Detection Systems are available to identify and protect the WLAN from attacks. The Wi-Fi Alliance certifies 802.11i devices under WPA2.

Wireless Client Association

In the client association process, access points send out beacons announcing one or more SSIDs, data rates, and other information. The client sends out a probe and scans all the channels and listens for beacons and responses to the probes from the access points. The client associates to the access point that has the strongest signal. If the signal becomes low, the client repeats the scan to associate with another access point (this process is called roaming). During association, the SSID, MAC address, and security settings are sent from the client to the access point and checked by the access point. Figure 3-6 illustrates the client association process.

Figure 3-6 *Client Association*



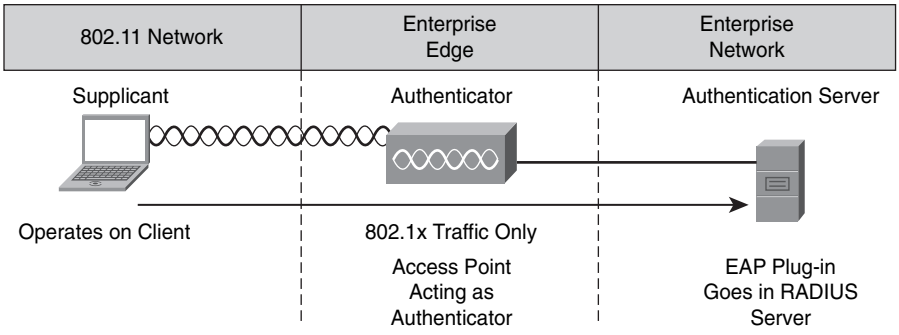
A wireless client's association to a selected access point is actually the second step in a two-step process. First, authentication and then association must occur before an 802.11 client can pass traffic through the access point to another host on the network. Client authentication in this initial process is not the same as network authentication (entering username and password to get access to the network). Client authentication is simply the first step (followed by association) between the wireless client and access point, and it establishes communication. The 802.11 standard specifies only two different methods of authentication: open authentication and shared key authentication. Open authentication is simply the exchange of four "hello" type packets with no client or access point verification, to allow ease of connectivity. Shared key authentication uses a statically defined WEP key, known between the client and access point, for verification. This same key might or might not be used to encrypt the actual data passing between a wireless client and an access point based on user configuration.

How 802.1x Works on WLANs

The access point, acting as the authenticator at the enterprise edge, allows the client to associate using open authentication. The access point then encapsulates any 802.1x traffic bound for the authentication server and sends it to the server. All other network traffic is blocked, meaning that all other attempts to access network resources are blocked. Figure 3-7 shows how 802.1x functions on a wireless network.

Upon receiving RADIUS traffic bound for the client, the access point encapsulates it and sends the information to the client. Although the server authenticates the client as a valid network user, this process allows the client to validate the server as well, ensuring that the client is not logging into a phony server.

Figure 3-7 *802.1x Authentication*



While an enterprise network uses a centralized authentication server, smaller offices or business might simply use the access point with preshared keys as the authentication server for wireless clients.

WPA and WPA2 Modes

WPA provides authentication support via 802.1x and a preshared key (PSK); 802.1x is recommended for enterprise deployments. WPA provides encryption support via TKIP. TKIP includes MIC and per-packet keying (PPK) via initialization vector hashing and broadcast key rotation.

In comparison to WPA, WPA2 authentication is not changed, but the encryption used is AES-Counter with CBC MAC Protocol (AES-CCMP). Table 3-2 compares the two WPA modes.

Table 3-2 *WPA Modes*

	WPA	**WPA2**
Enterprise Mode (Business, Education, Government)	Authentication: IEEE 802.1x/ EAP Encryption: TKIP/MIC	Authentication: IEEE 802.1x/ EAP Encryption: AES-CCMP
Personal Mode (SOHO, Home/Personal)	Authentication: PSK Encryption: TKIP/MIC	Authentication: PSK Encryption: AES-CCMP

Enterprise Mode

Enterprise Mode is a term given to products that are tested to be interoperable in both PSK and 802.1x/Extensible Authentication Protocol (EAP) modes of operation for authentication.

When 802.1x is used, an authentication, authorization, and accounting (AAA) server (the Remote Authentication Dial-In User Service (RADIUS) protocol for authentication and key management and centralized management of user credentials) is required. Enterprise Mode is targeted to enterprise environments.

NOTE While Cisco configuration typically uses RADIUS for authentication, the IEEE standard supports RADIUS, Terminal Access Controller Access Control System (TACACS+), DIAMETER, and Common Open Policy Service (COPS) as AAA services.

Personal Mode

Personal Mode is a term given to products tested to be interoperable in the PSK-only mode of operation for authentication. It requires manual configuration of a preshared key on the AP and clients. PSK authenticates users via a password, or identifying code, on both the client station and the AP. No authentication server is needed. Personal Mode is targeted to SOHO environments.

Summary of Understanding WLAN Security

The following summarizes the key points that were discussed in this lesson:

- With 802.1x, the access point, acting as the authenticator at the enterprise edge, allows the client to associate using open authentication.
- WPA provides authentication support via IEEE 802.1x and PSK.
    - Enterprise Mode is a term given to products that are tested to be interoperable in both PSK and IEEE 802.1x/EAP modes of operation for authentication.
    - Personal Mode is a term given to products tested to be interoperable in the PSK-only mode of operation for authentication.

Implementing a WLAN

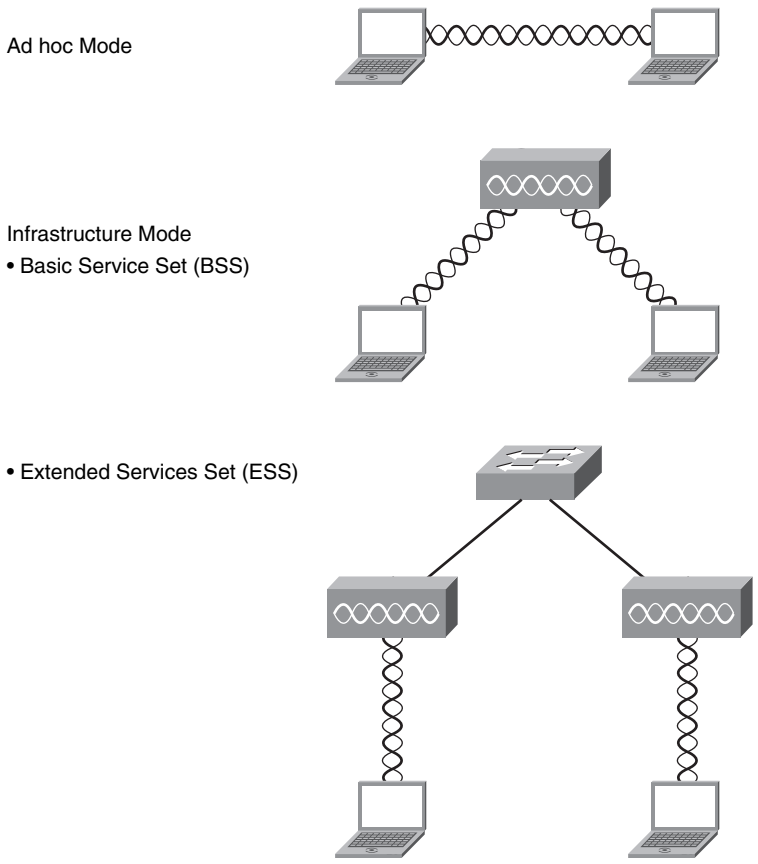
Implementing a WLAN involves more than selecting the desired standard and selecting a security mechanism. Access point placement can have more effect on throughput than standards. You need to understand how the efficiency of a WLAN is affected by such issues as topology, distance, and access point location.

Upon completing this lesson, you will be able to describe the factors affecting the implementation of a WLAN.

802.11 Topology Building Blocks

Figure 3-8 shows the original standard-defined 802.11 topologies: workgroup (ad hoc), infrastructure, and Extended Services Set. The other topologies such as repeaters, bridges, and workgroup bridges are vendor-specific extensions.

Figure 3-8 *802.11 Building Blocks*



The following list describes these different building blocks.

- **Ad hoc mode:** Independent Basic Service Set (IBSS) is the ad hoc topology mode. Mobile clients connect directly without an intermediate access point. Operating systems such as Windows have made this peer-to-peer network easy to set up. This setup can be used for a small office (or home office) to allow a laptop to be connected to the main PC or for several people to simply share files. The coverage is limited. Everyone must be able to hear everyone else. An access point is not required. A drawback of peer-to-peer networks is that they are difficult to secure.

- **Infrastructure mode:** In infrastructure mode, clients connect through an access point. There are two infrastructure modes:
  - **Basic Service Set (BSS):** The communication devices that create a BSS are mobile clients using a single access point to connect to each other or to wired network resources. The Basic Service Set Identifier (BSSID) is the Layer 2 MAC address of the BSS access point's radio card. While the BSS is the single building block for wireless topology and the BSS access point is uniquely identified through a BSSID, the wireless network itself is advertised through a SSID, which announces the availability of the wireless network to mobile clients. The SSID is a wireless network name that is user configurable and can be made up of as many as 32 case-sensitive characters.
  - **Extended Services Set (ESS):** The wireless topology is extended with two or more BSSs connected by a distribution system (DS) or a wired infrastructure. An ESS generally includes a common SSID to allow roaming from access point to access point without requiring client configuration.

BSA Wireless Topology

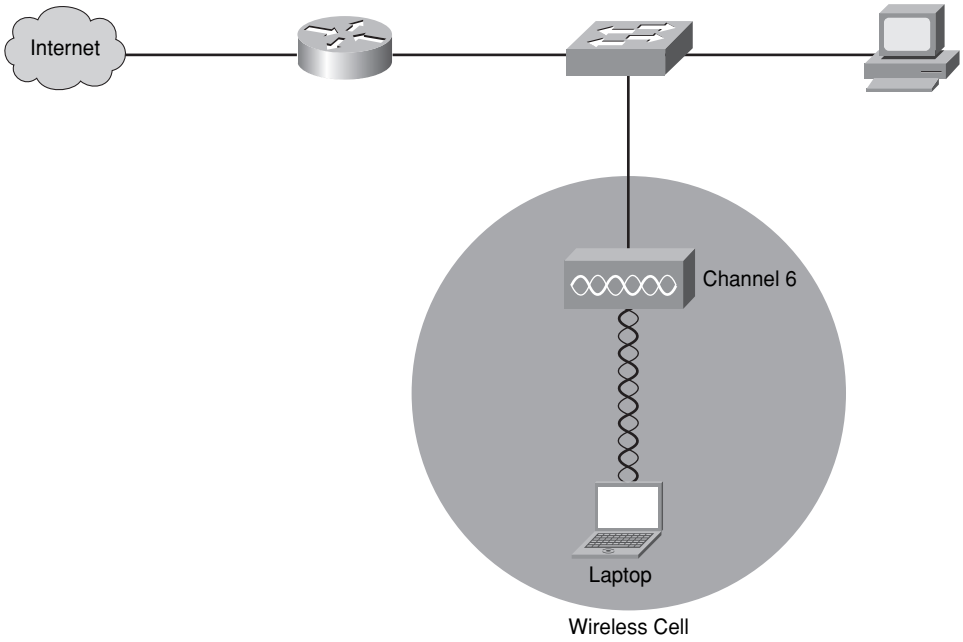
A Basic Service Area (BSA) is the physical area of RF coverage provided by an access point in a BSS. This area is dependent on the RF created with variations caused by access point power output, antenna type, and physical surroundings affecting the RF. While the BSS is the topology building block and the BSA is the actual coverage pattern, the two terms are used interchangeably in basic wireless discussions. Figure 3-9 shows a BSA topology.

The access point attaches to the Ethernet backbone and communicates with all the wireless devices in the cell area. The access point is the master for the cell and controls traffic flow to and from the network. The remote devices do not communicate directly with each other; they communicate only with the access point. The access point is user-configurable with its unique RF channel and wireless SSID name.

The access point broadcasts the name of the wireless cell in the SSID through beacons. Beacons are broadcasts that access points send to announce the available services. It is used to logically separate WLANs. It must match exactly between the client and the access point. However, clients can be configured without an SSID (null-SSID), then detect all access points, and learn the SSID from the beacons of the access points. A common example of the discovery process is the one used by the integrated Windows Zero Configuration (WZC) utility when a wireless laptop is used at a new location. The user is shown a display of the

newly found wireless service and asked to connect or supply appropriate keying material to join. SSID broadcasts can be disabled on the access point, but this approach does not work if the client needs to see the SSID in the beacon.

Figure 3-9 *BSA Topology*



If a single cell does not provide enough coverage, any number of cells can be added to extend the range. This range is known as an Extended Service Area (ESA). Figure 3-10 shows an ESA topology.

It is recommended that ESA cells have 10 to 15 percent overlap to allow remote users to roam without losing RF connections. For wireless voice networks, an overlap of 15 to 20 percent is recommended. Bordering cells should be set to different nonoverlapping channels for best performance.

Wireless Topology Data Rates

WLAN clients have the ability to shift data rates while moving. This strategy allows the same client operating at 11 Mbps to shift to 5.5 Mbps, then 2 Mbps, and finally still communicate in the outside ring at 1 Mbps. This rate-shifting happens without losing the connection and without any interaction from the user. Rate-shifting also happens on a transmission-by-transmission basis; therefore, the access point has the ability to support multiple clients at multiple speeds depending upon the location of each client. Figure 3-11 shows data rates at different distances from the access point.

Figure 3-10 *ESA Topology*

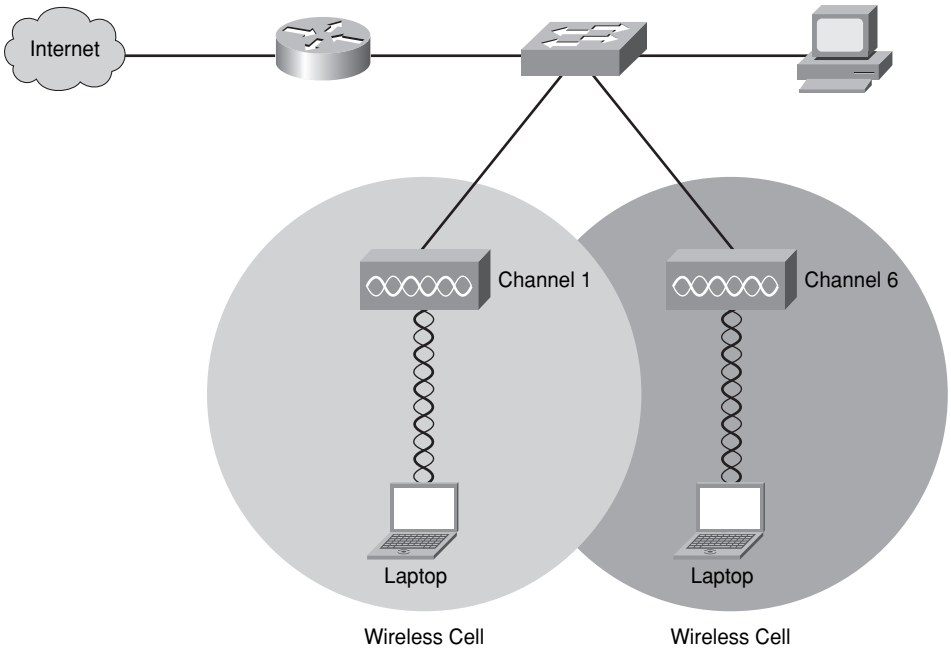
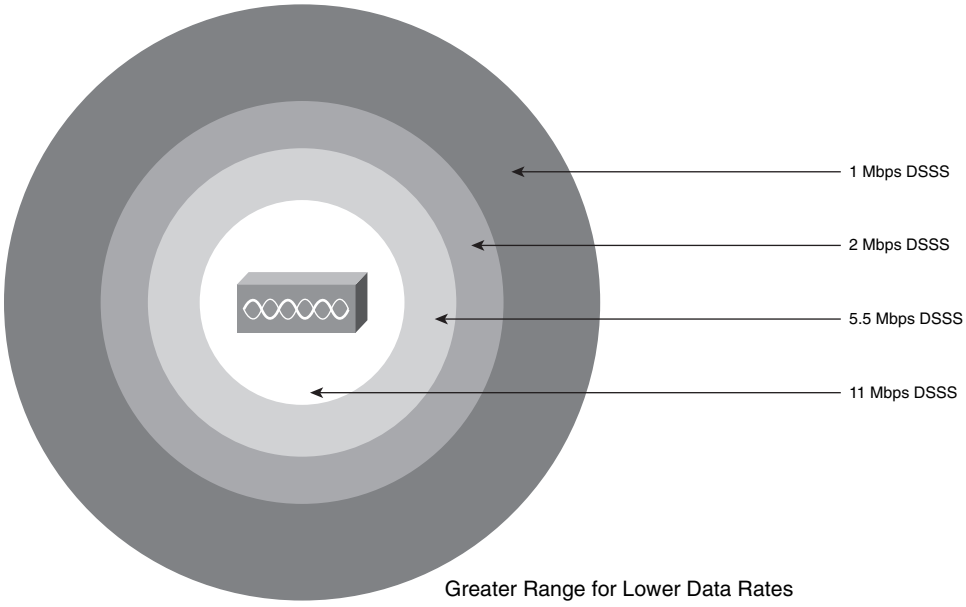


Figure 3-11 *Wireless Data Rates*



The following outlines the characteristics of data rates as they apply to client devices and signal strength:

- Higher data rates require stronger signals at the receiver. Therefore, lower data rates have a greater range.
- Wireless clients always try to communicate with the highest possible data rate.
- The client reduces the data rate only if transmission errors and transmission retries occur.

This approach outlined in the previous list provides the highest total throughput within the wireless cell. Figure 3-11 is for IEEE 802.11b; however, the same concept applies to IEEE 802.11a or IEEE 802.11g data rates.

Access Point Configuration

This topic describes the factors that should be considered when implementing a WLAN.

Wireless access points can be configured through a command-line interface (CLI), or more commonly through a browser GUI. However, the mode of configuration of the basic wireless parameters is the same. Basic wireless access point parameters include SSID, RF channel with optional power, and authentication (security), whereas basic wireless client parameters include only authentication. Wireless clients need fewer parameters because a wireless network interface card (NIC) scans all the available RF it can to locate the RF channel (meaning an IEEE 802.11b/g card cannot scan 5 GHz) and usually initiates the connection with a null-SSID to discover the available SSIDs. Therefore, by 802.11 design, if you are using open authentication, the result is plug-and-play. When security is configured with PSKs for older WEP or current WPA, remember that the key must be an exact match to allow connectivity.

Depending on the hardware chosen for the access point, it might be capable of two frequencies, 2.4 GHz ISM band and 5 GHz UNII band, and all three IEEE 802.11a/b/g implementations. The features of the access point usually allow for fine adjustment of parameters such as which frequencies to offer, which radio to enable, and which IEEE standard to use on that RF.

When 802.11b wireless clients are mixed with 802.11g wireless clients, throughput is decreased because the access point must implement a protection RTS/CTS protocol. Hence, if you implement only one IEEE wireless client type, throughput is greater than if you use a mixed mode.

After you configure the basic required wireless parameters of the access point, additional fundamental wired side parameters must be configured for the default router and Dynamic Host Configuration Protocol (DHCP) server. Given a pre-existing LAN, a default router is

needed to exit the network, and a DHCP server is needed to lease IP addresses to wired PCs. The access point simply uses the existing router and DHCP servers for relaying IP addresses to wireless clients. Because the network has been expanded, verify that the existing DHCP IP address scope is large enough to accommodate the new wireless client additions. If this is a new installation with all router and access point functions in the same hardware, then you simply configure all parameters in the same hardware.

Steps to Implement a Wireless Network

The basic approach to wireless implementation (as with any basic networking) is to gradually configure and test incrementally, following these steps:

Step 1 Before implementing any wireless, verify pre-existing network and Internet access for the wired hosts.

Step 2 Implement wireless with only a single access point and a single client, without wireless security.

Step 3 Verify that the wireless client has received a DHCP IP address and can ping the local wired default router and then browse to the external Internet.

Step 4 Finally, configure wireless security with WPA/WPA2. Only use WEP if hardware equipment does not support WPA/WPA2.

Wireless Clients

Currently, many form factors exist to add wireless to existing laptops. The most common are Universal Serial Bus (USB) devices with self-contained fixed antenna software and wireless supplicant software, both of which enable wireless hardware usage and provide security options for authentication and encryption. Most new laptops contain some form of wireless. This availability of wireless technology has increased the wireless market and improved ease of use. Newer Windows operating systems have a basic wireless supplicant client (WZC). WZC enables wireless plug-and-play by discovering SSIDs being broadcasted and allowing the user to simply type the matching security PSK for such items as WEP or WPA. The basic features of WZC satisfy more simple SOHO environments.

Large enterprise networks require more advanced wireless client features than those of native operating systems. In 2000, Cisco started a program of value-add feature enhancements through a royalty-free certification program. Over 95 percent of Wi-Fi–enabled laptops shipped today are Cisco Compatible Extensions compliant. The details and status of versions and features can be found on http://www.cisco.com/go/ciscocompatible/wireless. Table 3-3 shows a summary of versions and features:

Table 3-3 *Versions and Features*

Version	Topic	Example
V1	Security	Wi-Fi compliant; 802.1x, LEAP, Cisco Key Integrity Protocol
V2	Scaling	WPA, access point–assisted roaming
V3	Performance and security	WPA2, Wi-Fi Multimedia (WMM)
V4	Voice over WLAN	Call Admission Control (CAC), voice metrics, UPSD
V5	Management and IPS	Management Frame Protection (MFP), client reporting

Enterprise networks typically manage one set of wired clients and another set of wireless clients. Cisco offers a full-featured supplicant for both wired and wireless clients called Cisco Secure Services Client. The benefit to users is a single client for wired or wireless connectivity and security.

See http://www.cisco.com/go/ciscocompatible/wireless for additional information.

Wireless Troubleshooting

If you follow the recommended steps for implementing a wireless network, the divide-and-conquer technique via incremental configuration will most likely lead to a problem. These are the most common causes of configuration problems:

- Configuring a defined SSID on the client (versus its discovery method of SSID) that does not match the access point (inclusive of case sensitivity)
- Configuring incompatible security methods

Both the wireless client and access point must match for authentication method, EAP or PSK, and encryption method (TKIP or AES).

Other common problems resulting from initial RF installation can sometimes be identified by answering the following questions:

- Is the radio enabled on both the access point and client for the correct RF (2.4 GHz ISM or 5 GHz UNII)?
- Is an external antenna connected and facing the correct direction (straight upward for dipole)?
- Is the antenna location too high or too low relative to wireless clients (within 20 vertical feet)?
- Are there metal objects in the room reflecting RF and causing poor performance?
- Is the AP the client is attempting to reach at too great of a distance?

The first step in troubleshooting a suspected wireless issue is to break the environment into wired network versus wireless network. Then, further divide the wireless network into configuration versus RF issues. Begin by verifying the proper operation of the existing wired infrastructure and associated services. Verify that other pre-existing Ethernet-attached hosts can renew their DHCP addresses and reach the Internet.

Then co-locate both the access point and wireless client together to verify configuration and eliminate the possibility of RF issues. Always start the wireless client on open authentication and establish connectivity. Then, implement the desired wireless security.

If the wireless client is operational at this point, then only RF-related issues remain. First, consider whether metal obstructions exist. If so, move the obstruction or change the location of the access point. If the distance is too great, consider adding another access point using the same SSID, but a unique RF channel. Lastly, consider the RF environment. Just as a wired network can become congested with traffic, so can RF for 2.4 GHz (more often than 5 GHz). Check for other sources of wireless devices using 2.4 GHz.

If performance issues seem to relate to time of day, that would indicate RF interference from a device. An example would be slow performance at lunchtime in an office located near a microwave oven used by employees. While most microwaves jam RF channel 11, other microwaves jam all RF channels. Another cause of problems could be RF devices that hop frequencies, such as Frequency Hopping Spread Spectrum (FHSS) used in cordless phones. Because there can be many sources of RF interference, always start with co-locating the access point and wireless client and then move the wireless client until you can reproduce the problem. Most wireless clients have supplicant software that helps troubleshoot by presenting relative RF signal strength and quality.

Summary of Implementing a WLAN

The following summarizes the key points that were discussed in this lesson:

- Ad hoc mode: Clients connect directly without an intermediate access point.
- Infrastructure mode: Clients connect through an access point. There are two modes:
  - Basic Service Set (BSS)
  - Extended Services Set (ESS)
- BSS wireless topology:
  - Basic Service Area (BSA)
  - Extended Service Area (ESA)

- Wireless access points can be configured through a command-line interface or more commonly a browser GUI.
- The basic approach to wireless implementation is to gradually configure and test incrementally.
- Currently, many form factors exist to add wireless to existing laptops:
  - Windows Zero Configuration
  - Cisco Compatible Extensions
  - Cisco Secure Services Client
- Troubleshooting wireless by breaking the environment into wired network versus wireless network.

Chapter Summary

The different 802.11 standards identify the characters of the transmissions used by WLANs, while the Wi-Fi certification ensures compatibility between devices.

To address common threats to WLAN services, security has evolved to include 802.1x and WPA/WPA2.

Wireless implementations are affected by distance, speed, and form factors.

Review Questions

Use the questions here to review what you learned in this chapter. The correct answers can be found in the appendix, "Answers to Chapter Review Questions."

1. What is the most tangible benefit of wireless implementation?
   a. Cost reduction
   b. Increased mobility
   c. Better productivity
   d. Improved security

2. What method does a WLAN use to control transmissions?
   a. CSMA/CA (carrier sense multiple access with collision avoidance)
   b. CSMA/CD (carrier sense multiple access collision detect)

c. CSMA/CR (carrier sense multiple access with collision rejection)

d. CSMA/CW (carrier sense multiple access with collision weighting)

3. Match each factor that influences the transmission of radio waves to its correct description.

___Occurs when RF waves bounce off metal or glass surfaces

___Occurs when RF waves are soaked up by walls

___Occurs when RF waves strike an uneven surface and are reflected in many directions

a. absorption

b. reflection

c. scattering

4. Which regulatory agency controls the 801.11 standard that governs WLANs?

a. Wi-Fi Alliance

b. IEEE

c. EMA

d. WISC

5. Which organization offers certification for interoperability among vendors of 802.11 products?

a. Wi-Fi

b. IEEE

c. EMA

d. WISC

6. Which two are the unlicensed bands used by WLANs?

a. 2.4-MHz band

b. 900-MHz band

c. 2.4-GHz band

d. 5-GHz band

e. 900-GHz band

7. Which two of the 802.11 standards has the highest possible data rates?
   a. 802.11
   b. 802.11a
   c. 802.11b
   d. 802.11d
   e. 802.11g

8. Which 802.11 standard transmits using the 5-GHz band?
   a. 802.11
   b. 802.11a
   c. 802.11b
   d. 802.11d
   e. 802.11g

9. Which is true about the Wi-Fi Alliance organization?
   a. It is a global standards organization that controls the compatibility of Wi-Fi products.
   b. It operates only in the United States and ensures the compatibility of Wi-Fi products.
   c. It is a global, nonprofit industry trade association devoted to promoting the growth and acceptance of wireless LANs.
   d. It is a global, nonprofit industry trade association devoted to promoting the installation of wireless LANs in retail locations.

10. What is a rogue access point?
    a. An access point that has an open WEP key
    b. An access point that is broadcasting its SSID
    c. An unsecured access point that has been placed on a WLAN
    d. An access point that has had a hardware failure that causes it to endlessly broadcast its SSID

11. Which three are the steps to secure a WLAN?
    a. Encryption for providing privacy and confidentiality
    b. Authentication to ensure that legitimate clients and users access the network via trusted access points

c. Controls to transmit power to limit the access point access range to the property boundaries of the parent organization

d. Protection from security risks and availability with intrusion detection and intrusion protection systems for WLANs

12. Which standard provides the strongest level of WLAN security?

a. EAP

b. WEP

c. WPA

d. 802.11i/WPA2

13. What factor determines which access point a client associates with?

a. The access point with the lowest SSID

b. The access point with the highest SSID

c. The access point whose SSID is received first

d. The access point that is received with the strongest signal

14. When you are using 802.11x, how is the client authenticated?

a. The client is authenticated against a local database stored on the access point.

b. The access point forwards all network traffic to the server where it is either authenticated or blocked.

c. The access point encapsulates any 802.1x traffic bound for the authentication server and sends it to the server.

d. The client encapsulates the 802.1x authentication traffic before sending it to the access point. This causes the access point to forward it to the server.

15. Which is true when comparing WPA and WPA2?

a. WPA uses preshared keys whereas WPA 2 uses PSK.

b. WPA uses EAP authentication whereas WPA 2 uses 802.11x.

c. WPA uses a Personal Mode whereas WPA 2 uses an Enterprise Mode.

d. WPA uses TKIP/MIC encryption whereas WPA 2 uses AES-CCMP encryption.

16. Match each of the following 802.11 topologies to its description.

    ___Mobile clients connect directly without an intermediate access point.

    ___The communication devices use a single access point for connectivity to each other or to wired network resources.

    ___The wireless topology is two or more service sets connected by a distribution system (DS) or, more commonly, a wired infrastructure.

    a. Ad hoc mode
    b. Basic Service Set (BSS)
    c. Extended Services Set (ESS)

17. What does the physical area of radio frequency coverage provided by an access point define?

    a. The RF service area
    b. The basic service area
    c. The ad hoc service area
    d. The extended services area

18. When implementing Extended Service Areas, how much overlap is suggested?

    a. 5 to 10 percent
    b. 10 to 15 percent
    c. 15 to 20 percent
    d. 25 to 30 percent

19. What strategy enables a client to communicate while moving?

    a. The ability to shift data rates
    b. The ability to vary transmit levels
    c. The ability to match the transmit level to the receive level
    d. The ability to perform error correction as the signal level changes

20. Which three are basic wireless access point parameters?

    a. SSID
    b. Authentication

c. Data exchange rates
d. Transmit band selection
e. RF channel with optional power

21. When implementing a WLAN, when should you use WEP?

a. Only if an AAA server is available
b. When you need the increased security of WEP
c. When you are planning to enable 802.11x authentication
d. Only if the hardware equipment does not support WPA

22. Match the wireless client to its description.

___Full-featured supplicant for both wired and wireless client

___Windows operating systems basic wireless supplicant client

___More advanced wireless client features than those of native operating system

a. WZC
b. Cisco Compatible Extensions
c. Cisco Secure Services Client