This chapter discusses how to design a wireless network, and includes the following sections:

- Making the Business Case
- Wireless Technology Overview
- Wireless Security
- Wireless Management
- Wireless Design Considerations

CHAPTER 5

Wireless LAN Design

This chapter discusses wireless LAN (WLAN) technology and describes how it improves mobility. After introducing WLANs as strategic assets to corporate networks, we discuss WLAN standards and components. The security and management of WLANs are explored, followed by design considerations for WLANs.

NOTE Appendix B, "Network Fundamentals," includes material that we assume you understand before reading the rest of the book. Thus, we encourage you to review any of the material in Appendix B that you are not familiar with before reading the rest of this chapter.

Making the Business Case

The popularity of WLANs is undeniable. The following three main driving forces play in favor of WLANs:

- Flexibility
- Increased productivity
- Cost savings compared to wired deployment

WLANs let users access servers, printers, and other network resources regardless of their location, within the wireless reach. This flexibility means that, for example, a user's laptop stays connected working from a colleague's cubicle, from a small meeting room, or from the cafeteria. Recognizing the benefits brought about by WLAN flexibility, businesses are now deploying WLANs in record numbers.

According to a 2003 NOP World research study,[1] WLAN users stayed connected to their corporate network 3.64 hours per day longer than their wired peers, thus increasing their productivity by 27 percent. Through the flexibility of WLANs, not only does the productivity go up, but the response times are also significantly improved.

The benefits of wireless mobility don't stop at laptops and personal digital assistants (PDAs). IP telephony and videoconferencing are also supported over WLANs, integrating quality of service (QoS) to ensure that the interactive traffic has priority over the less-time-sensitive data transfers.

Another significant benefit of WLANs is their low-cost deployment in locations where the costs of running LAN wire would be prohibitive. The total cost of ownership (TCO) of a WLAN is very low compared to the benefits they bring to an organization, providing that a WLAN is secured and managed properly.

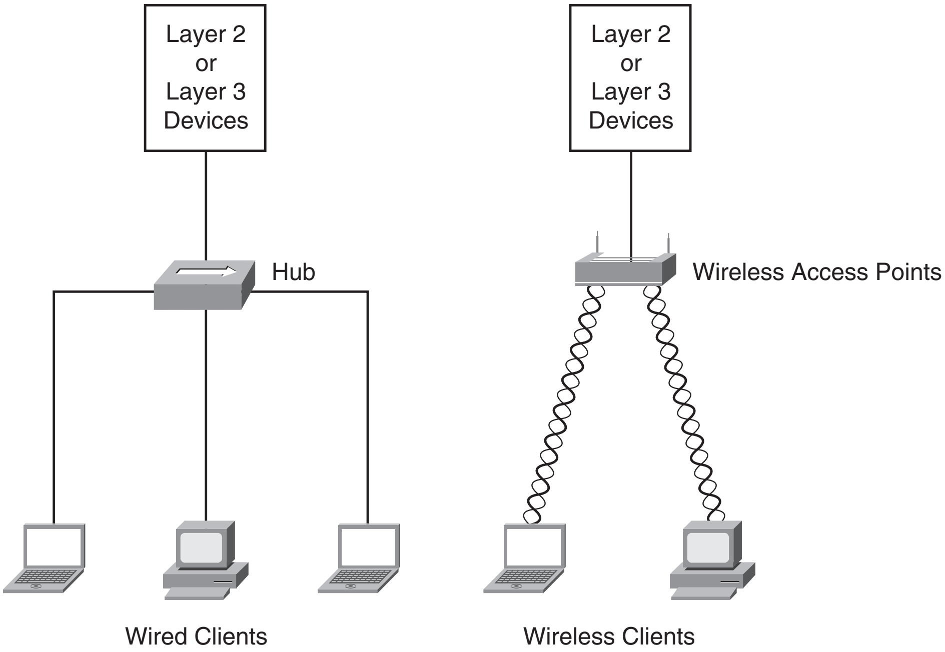
Companies that are not deploying WLANs quickly enough find that employees take the matter in their own hands and install their own WLANs, potentially creating significant breaches in the corporate network security infrastructure. Therefore, wireless security is an important topic to discuss in conjunction with wireless design.

WLANs, seen just a few years ago as a novelty, are now seen as critical to corporate productivity.

Wireless Technology Overview

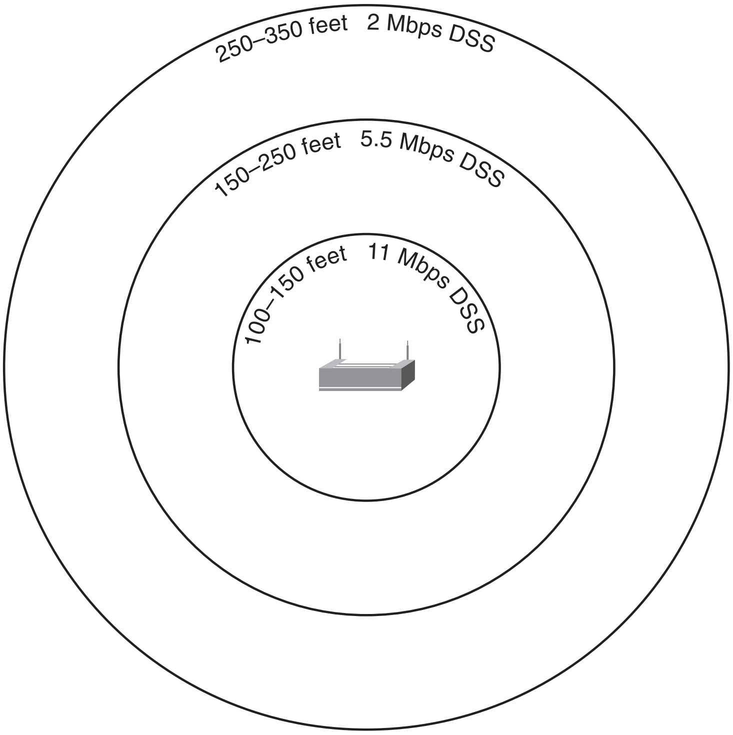
In its most simplistic form, a WLAN is an LAN that uses radio frequency (RF) to communicate instead of using a wire. As shown in Figure 5-1, wireless clients connect to wireless access points (WAPs).

Figure 5-1 *Wired and Wireless Networks*



Because WLANs use RF, the throughput (speed) is inversely proportional to the distance between the transmitter and the receiver.[2] Therefore, everything being equal (notwithstanding interferences), the closer a wireless client is to a transmitter, the greater is the throughput, as shown in Figure 5-2.

Figure 5-2 *Throughput (Coverage) Is Related to the Distance from the RF Transmitter*



DSS = Digital Spread Spectrum

However, wireless communication brings a trade-off between flexibility and mobility versus battery life and usable bandwidth.

Wireless Standards

WLAN standards that are currently supported by major vendors were developed by the working group 11 of the Institute of Electrical and Electronics Engineers (IEEE) 802 committee. The most common standards are shown in Table 5-1.

Table 5-1 *Wireless Standards*

Standard	Maximum Throughput (Mbps)	Frequency (GHz)	Compatibility	Ratified
802.11b	11	2.4	—	1999
802.11a	54	5	—	1999; Product availability 2001
802.11g	54	2.4	Backward-compatible with 802.11b	2003

The 802.11a standard operates in the unlicensed 5-GHz band, which makes the transmission vulnerable to interference from microwave ovens and cordless phones. The strength of 802.11b and 802.11g signals, which operate in the 2.4-GHz band, is affected negatively by water, metal, and thick walls.

The 802.11b and 802.11g standards divide the 2.4 GHz into 14 overlapping individual channels. Channels 1, 6, and 11 do not overlap and therefore can be used to set up multiple networks. The 802.11a standard is an amendment to the original standard. The advantage of using 802.11a is that it suffers less from interference, but its use is restricted to almost line of sight, thus requiring the installation of more access points than 802.11b to cover the same area.

The medium access method of the 802.11 standards, called the Distribution Coordination Method, is similar to the carrier sense multiple access collision detect (CSMA/CD) mechanism of Ethernet.

The following types of frames are transferred over the airwaves:

- **Data frame**—Network traffic.
- **Control frame**—Frame controlling access to the medium, similar to a modem's analog connection control mechanism, with its Request To Send (RTS), Clear To Send (CTS), and acknowledgment (ACK) signals.
- **Manager frame**—Frames similar to data frames, pertaining to the control of the current wireless transmission.

Other Wireless Standards

Other wireless standards include the following:

HomeRF—In 1998, a consortium was formed to promote the idea of HomeRF to be used with products in the home market. The participants were, among others, Siemens, Motorola, and Compaq.

Bluetooth—This is a specification for short-range radio links between mobile computers, mobile phones, digital cameras, and other portable devices, such as headsets. Bluetooth could be considered a standard for *personal area networks.*

Wireless Components

The main components of wireless networks are as follows:

- Wireless access points
- Wireless client devices

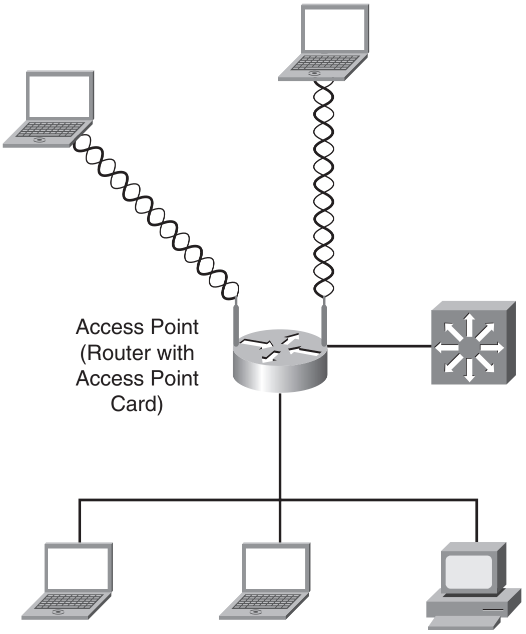
Wireless Access Points

WAPs provide connectivity between wireless client devices and the wired network, as shown earlier in Figure 5-1.

Integrated Access Point

The WAP does not need to be a stand-alone device. Cisco offers integrated access point functionality[3] for some small- to medium-business (SMB) routers, as shown in Figure 5-3. By installing a high-speed wireless interface card (HWIC) in Cisco 1800, 2800, or 3800 routers, customers can run concurrent routing, switching, and security services and include IEEE 802.11 wireless LAN functionality in a single platform.

Figure 5-3 *Integrating Routing and Wireless Functionality*



Wireless Client Devices

A wireless client device is equipped with a wireless interface card (WIC), which the device uses to communicate over RF with WAPs. Wireless clients can be the following items, among other things:

- User workstations and laptops
- PDAs
- Wireless IP phones

User Workstations and Laptops: Ad-Hoc Network

In addition to connecting to a WLAN access point, two wireless end stations can form an exclusive, point-to-point, wireless network without the intervention of an access point. This type of independent network is known as an *ad-hoc network.*

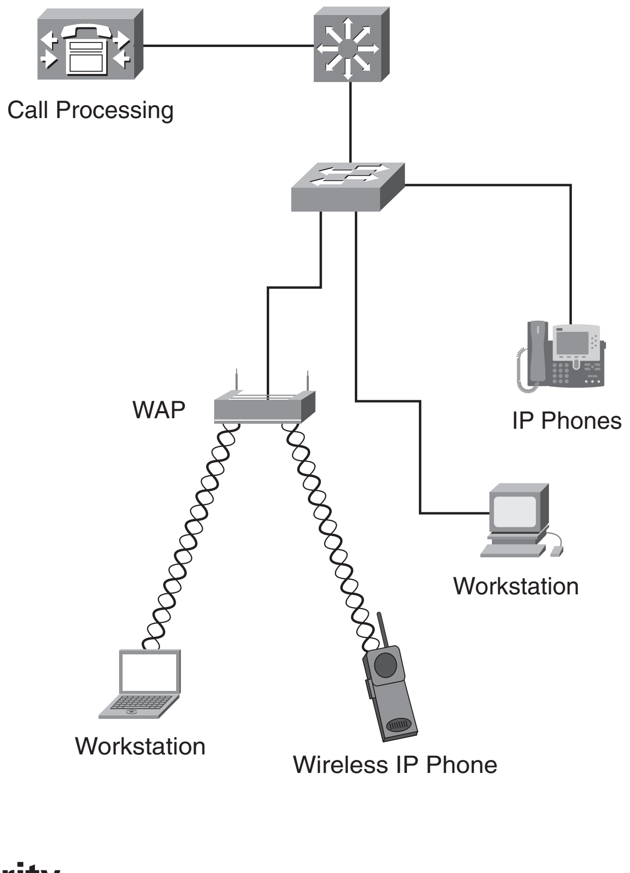
PDAs

Wireless PDAs—PDAs that connect directly on the corporate network—play a significant role in an organization where time is extremely sensitive. An example of where 802.11b-compatible devices (wireless PDAs) are put to benefit is triage nurses who are faster at inputting their assessment and sharing their findings on the spot rather than walking back to the nurses' station to do so.

Wireless IP Phones

Absolute campus mobility is probably best demonstrated by Cisco wireless IP phones.[4] These 802.11b phones have built-in security, QoS, and management features. Wireless IP phones leverage existing IP telephony deployments, as shown in Figure 5-4.

Figure 5-4 *Deploying Wireless IP Phones*



Wireless Security

Although security was originally included with 802.11 standards, it soon became obvious that it wasn't enough. Wireless security—or the lack of it—has been a major contributor to IT managers' reluctance to adapt wireless LANs.

Recently, wireless security has improved dramatically, providing IT managers with an acceptable level of comfort to proceed with the installation of WLANs. IEEE 802.11i, released in June 2004, addresses current security concerns.

In addition to the 802.11 suite of standards, the 802.1x standard can be used for wireless security. More precisely, 802.1x addresses port-based access control.

Wireless Security Issues

A main issue with wireless communication is unauthorized access to network traffic or, more precisely, the watching, displaying, and logging of network traffic, also known as *sniffing.* Contrary to a wired network, where a hacker would need to be physically located at the corporate premises to gain access through a network drop, with a wireless network, the intruder can access the network from a location outside the corporate building. WLANs use radio frequencies, and their signals propagate through ceilings and walls. Therefore, wireless eavesdropping, known as *war driving* or *walk-by hacking,* and rogue WAPs—unauthorized WAPs that allow a hacker access to a network—are two significant security issues with wireless networks.

Moreover, wireless equipment tends to ship with open access. Not only is traffic propagated in clear text, but WAPs also voluntarily broadcast their identity, known as Service Set Identifiers (SSIDs).

Wireless Threat Mitigation

Thanks to the wireless open-access default mode, we can join a wireless network from our favorite coffee shop or hotel room; however, this unrestricted access is not advisable for corporate networks. Wireless network security can be classified into the following three categories:

- Basic wireless security
- Enhanced wireless security
- Wireless intrusion detection

Basic Wireless Security

Basic wireless security is provided by the following built-in functions:

- SSIDs
- Wired Equivalent Privacy (WEP)
- Media Access Control (MAC) address verification

SSIDs

An SSID is a code that identifies membership with a WAP. All wireless devices that want to communicate on a network must have their SSID set to the same value as the WAP SSID to establish connectivity with the WAP.

By default, a WAP broadcasts its SSID every few seconds. This broadcast can be stopped so that a drive-by hacker can't automatically discover the SSID and hence the WAP. However, because the SSID is included in the beacon of every wireless frame, it is easy for a hacker equipped with sniffing equipment to discover the value and fraudulently join the network.

Beacon Frame

The WAP periodically advertises SSID and other network information using a special 802.11 management frame known as a *beacon.*

Being able to join a wireless network by the mere fact of knowing the SSID is referred to as *open authentication.*

Wired Equivalent Privacy

WEP can be used to alleviate the problem of SSID broadcasts by encrypting the traffic between the wireless clients and WAPs. Joining a wireless network using WEP is referred to as *shared-key authentication,* where the WAP sends a challenge to the wireless client who must return it encrypted. If the WAP can decipher the client's response, the WAP has the proof that the client possesses valid keys and therefore has the right to join the wireless network. WEP comes in two encryption strengths: 64-bit and 128-bit.

NOTE Even if a user manages to proceed with open authentication—for example, he guesses the SSID—if WEP is activated, he could not communicate with the WAP until he obtains the keys.

However, WEP is not considered secure: A hacker sniffing first the challenge and then the encrypted response could reverse-engineer the process and deduce the keys used by the client and WAP.

MAC Address Verification

To further wireless security, a network administrator could use MAC address filtering, in which the WAP is configured with the MAC addresses of the wireless clients that are to be permitted access.

Unfortunately, this method is also not secure because frames could be sniffed to discover a valid MAC address, which the hacker could then spoof.

Enhanced Wireless Security

Stronger security standards, shown in Table 5-2, were created to replace the weaknesses in WEP.

Table 5-2 *Wireless Security Standards*

Security Component	802.11 Original Standards	Security Enhancement
Authentication	Open authentication or shared-key	802.1x
Encryption	WEP	Wireless Fidelity (Wi-Fi) Protected Access (WPA), then 802.11i

802.1x

IEEE 802.1x is a port-based network access control standard. It provides per-user, per-session, mutual strong authentication, not only for wireless networks but also for wired networks, if need be.

Depending on the authentication method used, 802.1x can also provide encryption. Based on the IEEE Extensible Authorization Protocol (EAP), 802.1x allows WAPs and clients to share and exchange WEP encryption keys automatically. The access point acts as a proxy, doing the heavier computational load of encryption. The 802.1x standard also supports a centralized key management for WLANs.

Wi-Fi Protected Access

WPA was introduced as an intermediate solution to WEP encryption and data integrity insecurities while the IEEE 802.11i standard was being ratified.

When WPA is implemented, access to the WAP is provided only to clients that have the right passphrase. Although WPA is more secure than WEP, if the preshared key is stored on the wireless client and the client is stolen, a hacker could get access to the wireless network.

WPA supports both authentication and encryption. Authentication done through preshared keys is known as WPA Personal; when done through 802.1x, it is known as WPA Enterprise.

WPA offers Temporal Key Integrity Protocol (TKIP) as an encryption algorithm and a new integrity algorithm known as Michael. WPA is a subset of the 802.11i specification.

802.11i

In June 2004, the IEEE ratified the draft for the 802.11i standard, also known as WPA2. The 802.11i standard formally replaces WEP and other security features of the original IEEE 802.11 standard.

WPA2 is the *product certification* attributed to wireless equipment that is compatible with the 802.11i standard. WPA2 certification provides support for the additional mandatory 802.11i security features that are not included in WPA. WPA2, like WPA, supports both Enterprise and Personal modes for authentication.

In addition to stricter encryption requirements, WPA2 also adds enhancements to support fast roaming of wireless clients by allowing a client to preauthenticate with the access point toward which it is moving, while maintaining a connection to the access point that it is moving away from.

Wireless Intrusion Detection

Many products provide rogue access point detection. However, some third-party products integrate better than others with Cisco Aironet WAPs and the CiscoWorks Wireless LAN Solution Engine (WLSE), discussed in the next section. One such third-party product is from AirDefense.[5] This product provides wireless intrusion detection that uses the access points to scan the airwaves and report wireless activity.

Wireless Management

Wireless LANs require the same level of security, dependability, and management that wired networks do.

Network management tasks related to WLANs are as follows:

- RF management services
- Interference detection
- Assisted site survey
- RF scanning and monitoring

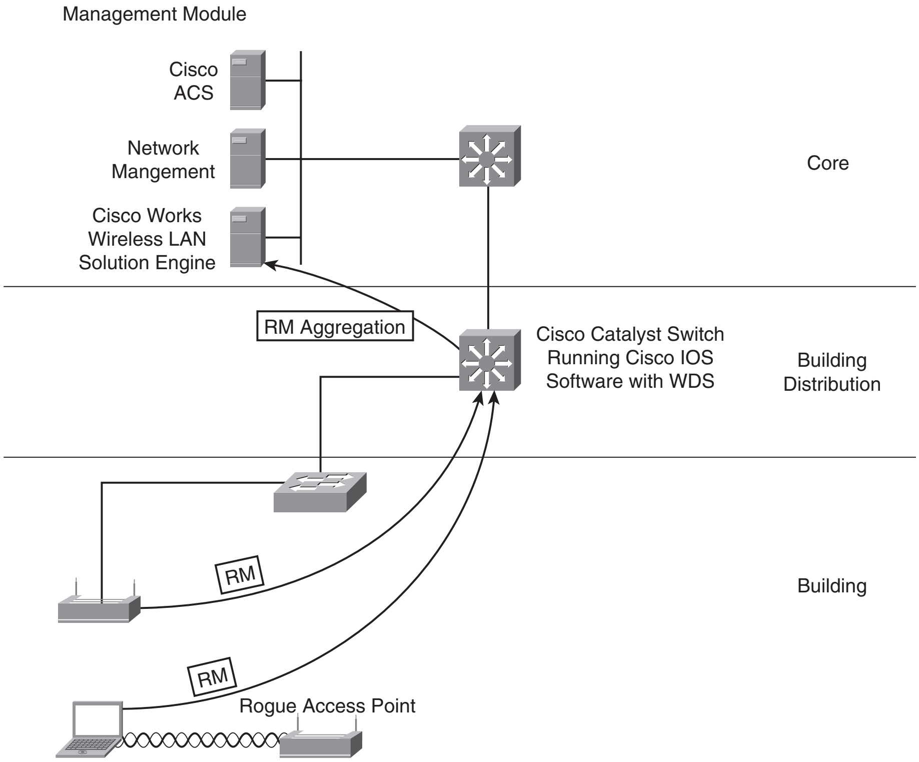
Cisco Integrated Wireless Network[6] is an evolution of the Cisco Structured Wireless-Aware Network (SWAN), which has been available from Cisco since 2003. The main components of Structured Wireless-Aware Networks[7] are as follows:

- Cisco Aironet WAP
- Management and security servers, specifically CiscoWorks WLSEs
- Wireless clients
- SWAN-aware Cisco Catalyst switches and Cisco routers

Cisco Integrated Wireless Network addresses wireless security, deployment, management, and control issues. It seeks to provide the same level of security, scalability, reliability, ease of deployment, and management for wireless LANs as is expected from wired LANs.

Cisco Integrated Wireless Network requires wireless clients to send RF management (RM) data to a Cisco Aironet WAP, Cisco IOS router, or Cisco Catalyst switch running Wireless Domain Services (WDS), as shown in Figure 5-5.

Figure 5-5 *Campus Infrastructure and Cisco Integrated Wireless Network*



The WDS devices aggregate all the RM data. All access points and clients register with WDS using 802.1x. The WDS devices forward the authentication information to a CiscoWorks WLSE.

One of the many benefits of WDS is Fast Secure Roaming, which assists a wireless client when migrating from one WAP to another. Another significant benefit of Cisco Integrated Wireless Network is the alert generated should a rogue WAP or rogue wireless client connect to the network, because all connecting devices are reported to the WDS device for further authentication.

Although they should be concerned with wireless security, organizations shouldn't forget the basics of physical security, as demonstrated by the following story. In 2005, a Middle Eastern bank was broken into. The thief didn't take anything, but rather left something—a WAP in the wiring closet connecting to the bank's LAN. The hacker was already *inside* the bank network and therefore effortlessly proceeded to transfer money until his stratagem was discovered.

Wireless Design Considerations

The following sections discuss some items that should be considered when designing and provisioning a wireless network.

Site Survey

Site surveys, originally introduced to make the most of scarce resources, are sometimes seen as unnecessary in this age of inexpensive WAPs, where wireless saturation seems so economical. Maybe the days of serious physical surveying, where one would look under the ceiling tiles, are long gone, but you should still perform surveying to determine the optimal locations for WAPs to minimize channel interference while maximizing the range.

Whether you are performing an in-depth site survey or a rudimentary one, you should ask the following questions:

- Which wireless system is best suited for the application?
- Does a line-of-sight requirement exist between antennas?
- Where should the WAP be located so that it is as close as possible to clients?
- What potential sources of interference are in this building? Example sources are cordless phones, microwave ovens, natural interference, or other access points using the same channel.
- Should any federal, provincial, or local regulations and legislation be considered in this deployment?

Site Surveys Have Their Purpose

Some WAPs have an autoconfiguration option with which, after listening on the network, they can autoconfigure themselves for the least-used wireless channel. This is not always desirable, though. For example, if a WAP is installed on the sixth floor of a multi-WAP, multistory building, it might select a channel that it perceived to be available. If that channel is already used by a WAP on the first floor, a client on the third floor could have difficulty staying connected because the channels overlap there.

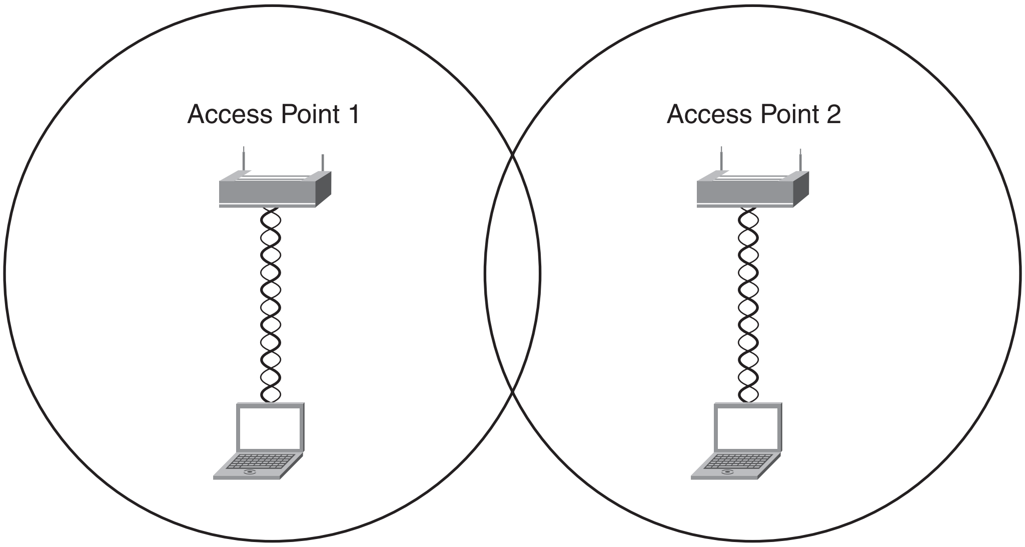
Overlapping channels in a wireless network perform similarly to an overcrowded wired network plagued by continuous collisions. Undoubtedly, performance will suffer and clients might not be able to establish consistent connectivity to the wireless network.

This problem could be more easily solved with rudimentary planning and by using nonoverlapping channels. Channels 1, 6, and 11 do not overlap, as mentioned in the "Wireless Standards" section, earlier in this chapter.

WLAN Roaming

WLANs are relatively inexpensive to deploy compared to wired networks, and because, as shown earlier in Figure 5-2, throughput is directly related to the proximity of WAPs, network managers often install WAPs to provide overlapping signals, as shown in Figure 5-6. Using this overlapping design, coverage (radius) area is traded for improved throughput.

Figure 5-6 *Overlapping Signals Eliminate Dead Spots*

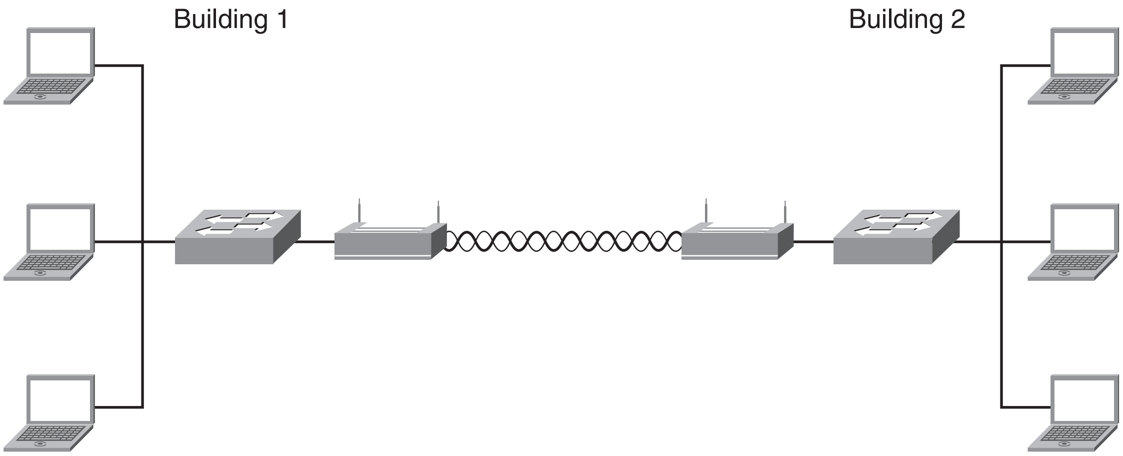


Note that these overlapping signals must be in nonoverlapping channels. This scenario, however, requires WLAN roaming. WLAN roaming plans consider that as a user moves away from a WAP and is therefore losing signal strength, his connection should seamlessly jump to a WAP that provides a stronger signal.

Point-to-Point Bridging

It is not always feasible to run a network cable between two buildings to join their respective LANs into a single Layer 3 broadcast domain. If the two buildings are a reasonable distance apart and preferably in direct line of sight with each other, wireless bridges can be configured, as shown in Figure 5-7. It takes two WAPs to create one logical two-port bridge. In this mode, WAPs are operating in a dedicated point-to-point bridge mode and therefore are no longer operating as wireless access points for clients.

Figure 5-7 *Point-to-Point Bridging*



Design Considerations for Wireless IP Phones

Because wireless IP phones have different coverage and wireless characteristics than common wireless clients, a system administrator should conduct another site survey.

Another consideration for wireless IP phones is roaming. The roaming described in the “WLAN Roaming” section, earlier in this chapter, is Layer 2 roaming. With Layer 2 roaming, devices keep their IP address and therefore the changing to another switch would not be noticeable by users. Layer 3 roaming would mean that a device would have to change its IP address; this would mean an interruption in the user’s connection. If the connection was to a wireless IP phone, the call would be disconnected; this scenario would likely be unacceptable to users. When wireless IP phones are used, the network needs to be equipped with a Cisco Catalyst 6500 Series Wireless LAN Services Module (WLSM). WLSM, an integral component of SWAN, provides aggregation of access point radio management information, thus enabling Layer 2 and Layer 3 roaming and client mobility management.

Layer 2 roaming refers to an IP phone switching WAP within its subnet of origin. Layer 3 roaming refers to an IP phone switching connectivity from a WAP in its subnet to a WAP located in another subnet. Prior to WLSM, Layer 3 roaming was an issue because the phone would end up in a subnet to which its IP address and default gateway wouldn't belong.

Summary

In this chapter, you learned about wireless technology and implementation. The following topics were covered:

- The prevalence and rapid growth of wireless networks
- Industry standards pertaining to wireless LANs
- Equipment comprising wireless LANs
- Wireless security and threat mitigation such as the following:
  - WEP
  - WPA and 802.11i
  - 802.1x
  - Wireless intrusion detection
- Wireless management using Cisco Integrated Wireless Networks
- Design considerations for wireless networks such as site surveys and roaming capabilities

Endnotes

[1] "Cisco Business Ready Campus Solutions" http:// www.cisco.com/application/pdf/en/us/ guest/netsol/ns431/c654/cdccont_0900aecd800d8124.pdf.

[2] "Wireless LANs At-A-Glance," Cisco 2004, http://www.cisco.com/application/pdf/en/us/guest/netsol/ns24/c643/cdccont_0900aecd800dc92e.pdf.

[3] "Cisco HWIC-AP WLAN Module for Cisco 1800 (Modular), 2800 and 3800." http://www.cisco.com/en/US/products/ps5949/products_data_sheet0900aecd8028cc7b.html.

[4] "Cisco Wireless IP Phone 7920," http://www.cisco.com/en/US/partner/products/hw/phones/ps379/ps5056/index.html.

[5] http://www.airdefense.net/cisco.

[6] "Cisco Integrated Wireless Network," http://www.cisco.com/en/US/netsol/ns340/ns394/ns348/ns337/networking_solutions_package.html.

[7] "Cisco Structured Wireless-Aware Network (SWAN) Multimedia Presentation." http://www.cisco.com/en/US/netsol/ns340/ns394/ns348/ns337/networking_solutions_presentation0900aecd8022d512.shtml.