Wireless LAN routers offer strong benefits in the home and small office setting. For example, you can subscribe to a cable modem service that provides a single IP address through DHCP to the router, and the router then provides IP addresses through DHCP to clients on your local network. NAT then maps a particular client on the local network to the ISP-assigned IP address whenever that client needs to access the Internet. As a result, you need a router if you plan to have more than one networked device on a local network sharing a single ISP-assigned address. Instead of having one box for the router and another box for the access point, a wireless LAN router provides both in the same box. Routers, however, are seldom used in larger implementations, such as hospitals and company headquarters. In these cases, access points are best because the network will have existing wired components that deal with IP addresses.

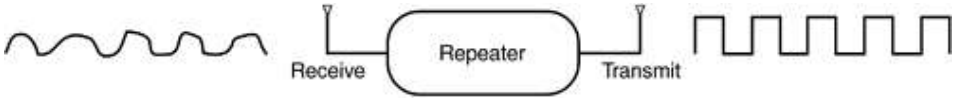
Repeaters

Access points, which require interconnecting cabling, generally play a dominant role for providing coverage in most wireless LAN deployments. Wireless **repeaters**, however, are a way to extend the range of an existing wireless LAN instead of adding more access points. There are few standalone wireless LAN repeaters on the market, but some access points have a built-in repeater mode.

A repeater simply regenerates a network signal to extend the range of the existing network infrastructure. (See **Figure 5-3**.) A wireless LAN repeater does not physically connect by wire to any part of the network. Instead, it receives radio signals from an access point, end-user device, or another repeater; it retransmits the frames. This makes it possible for a repeater located between an access point and distant user to act as a relay for frames traveling back and forth between the user and the access point.

Exhibit 1010
Page 150 of 292

Figure 5-3. Wireless LAN Repeaters Are Simple Devices That Require No Cabling



As a result, wireless repeaters are an effective solution to overcome signal impairments such as RF attenuation. For example, repeaters provide connectivity to remote areas that normally would not have wireless network access. An access point in a home or small office might not quite cover the entire area where users need connectivity, such as a basement or patio. The placement of a repeater between the covered and uncovered areas, however, will provide connectivity throughout the entire space. The wireless repeater fills holes in coverage, enabling seamless roaming.

A downside of wireless repeaters, however, is that they reduce performance of a wireless LAN. A repeater must receive and retransmit each frame on the same radio channel, which effectively doubles the amount of traffic on the network. This problem compounds when using multiple repeaters, because each repeater will duplicate the data sent. Therefore, be sure to plan the use of repeaters sparingly.

Antennae

Most antennae for wireless LANs are omnidirectional and have low gain. Nearly all access points, routers, and repeaters come standard with omnidirectional antennae. Omnidirectional antennae satisfy most coverage requirements; however, consider the use of optional directive antennae to cover a long, narrow area. In some cases, the antenna is integrated within a radio card or access point and there is no choice to make. If a need exists to use a directive antenna (higher gain), ensure that the radio card or access point has an external antenna connector.

Exhibit 1010
Page 151 of 292

Exhibit 1010
Page 152 of 292

Wireless LAN Systems

A wireless LAN system consists of a set of components and configurations that satisfy the needs of a particular application. It's possible to define a general wireless LAN system based on broad application types. Take a look at some examples.

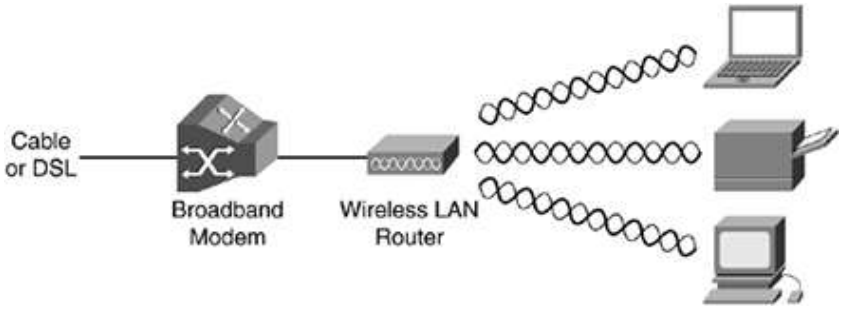
Home and Small Office Wireless LANs

The use of a wireless LAN in a home or small office avoids the need to run network cabling to interconnect PCs, laptops, and printers. Just about anyone can purchase applicable components at an electronics or office supply store and install a wireless LAN. Installation and configuration of the wireless LAN is simple.

As shown in **Figure 5-4**, a home or small office wireless LAN generally includes a single wireless LAN router that connects to a broadband Internet connection, such as DSL or cable modem. The typical range of a wireless LAN router is adequate to cover a house, apartment, or small office. A router is necessary if there is more than one network device. For example, a home consisting of one wireless PC, a laptop, and a printer requires NAT and DHCP to satisfy the addressing needs of all devices.

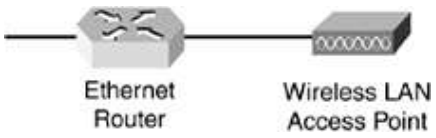
Figure 5-4. Wireless LANs in Home or Small Offices Have a Simple Configuration

Exhibit 1010
Page 153 of 292



An access point alone will also work in a home or small office, but it will allow only one network device to obtain an IP address and access the Internet. This occurs because most access points do not implement DHCP and NAT. The combination of an access point and wired router (see **Figure 5-5**), however, will suffice for a wireless LAN router. This might be a less expensive solution than purchasing a wireless LAN router if you already own an access point or wired router (or both).

Figure 5-5. Combining a Wireless LAN Access Point and an Ethernet Router Offers the Same Functionality of a Wireless LAN Router



tip



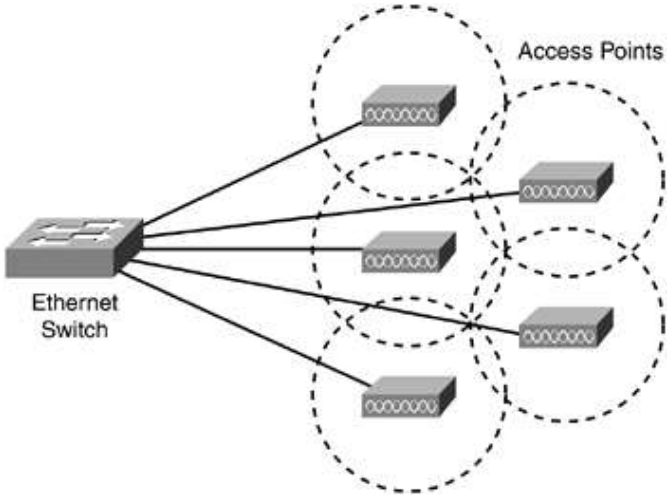
Wireless LAN access points and routers have default security settings, such as WEP, initially turned off. To prevent someone outside your home or office from accessing files on your network, activate security controls when setting up the wireless LAN.

Exhibit 1010
Page 154 of 292

Enterprise Wireless LANs

A wireless LAN for an enterprise is much more complicated than for homes and small offices. The main reason is that enterprise wireless LANs require multiple access points with the need of a substantial distribution system that interconnects the access points. As show in Figure 5-6, the access points offer overlapping radio cells that enable users to roam through a facility and access resources on a wired network. This configuration, often referred to as infrastructure mode, is the most common for any wireless LAN needing to cover an area greater than 20,000 square feet.

Figure 5-6. Enterprise Wireless LANs Require a Substantial Amount of Cabling to Interconnect Access Points



For example, a wireless LAN for a hospital might consist of hundreds of access points located throughout the hospital. A large array of Ethernet switches and associated cabling would be necessary to tie everything together. As with other enterprise wireless LANs, a hospital will likely have existing hardware that provides DHCP services. As a result, an enterprise wireless LAN utilizes access points, not wireless LAN routers.

Exhibit 1010
Page 155 of 292

Enterprise wireless LANs also require sophisticated security mechanisms. More emphasis must be placed on authentication and encryption than what is necessary for home and small office applications. Read **Chapter 8**, "Wireless Network Security: Protecting Information Resources," for more details on wireless LAN security.

tip



When deploying an enterprise or public wireless LAN, be certain to have a wireless LAN specialist perform an RF site survey to assess the presence of RF interference sources an and determine the optimum placement of access points and RF channel assignments.

Wireless LANs Good for Patients

Health-care centers, such as hospitals and doctors' offices, must maintain accurate records to ensure effective patient care. A simple mistake can cost someone's life. As a result, doctors and nurses must carefully record test results, physical data, pharmaceutical orders, and surgical procedures. This paperwork often overwhelms health-care staff, taking 50 to 70 percent of their time. The use of a mobile data collection device that wirelessly transmits the data to a centralized database significantly increases accuracy and raises the visibility of the data to those who need the information. This results in better care given to patients.
Doctors and nurses are also extremely mobile, going from room to room caring for patients. The use of electronic patient records, with the ability to input, view, and update patient data from anywhere in the hospital, increases the accuracy and speed of health care. This improvement is possi-

Exhibit 1010
Page 156 of 292

ble by providing each nurse and doctor with a wireless pen-based computer, such as a tablet or PDA, coupled with a wireless network to databases that store critical medical information about the patients.

A doctor caring for someone in the hospital, for example, can place an order for a blood test by keying the request into a handheld computer. The laboratory will receive the order electronically and dispatch a lab technician to draw blood from the patient. The laboratory will run the tests requested by the doctor and enter the results into the patient's electronic medical record. The doctor can then check the results through the handheld appliance from anywhere in the hospital.

Another application for wireless networks in hospitals is the tracking of pharmaceuticals. The use of mobile handheld bar code printing and scanning devices dramatically increases the efficiency and accuracy of all drug transactions, such as receiving, picking, dispensing, inventory taking, and the tracking of drug expiration dates. Most importantly, however, it ensures that hospital staff is able to administer the right drug to the right person in a timely fashion. This would not be possible without the use of wireless networks to support a centralized database and mobile data collection devices.

Public Wireless LANs

A **public wireless LAN** enables anyone with a wireless LAN NIC-equipped user device to access the Internet. Public wireless LANs are available from most hotpots, such as airports, convention centers, hotels, and marinas throughout the world. Good **hotspots** include those where people visit regularly on a temporary basis and want access to network services.

Exhibit 1010
Page 157 of 292

note



Locate a nearby public wireless LAN hotspot at **http://www.wi-fihotspotlist.com/**.

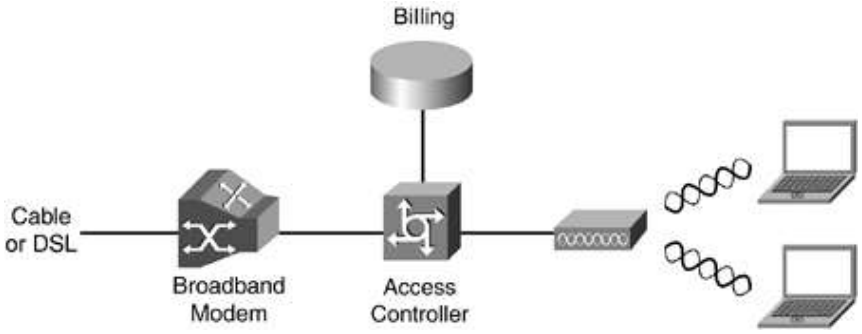
A public wireless LAN is one that anyone can use. This provides a source of revenue because the hotspot owner can bill subscribers. In some situations, though, hotspot owners offer free access in order to increase the use of their establishment.

Wireless LANs for small hotspots are simple. For example, a coffee shop owner can install a single wireless LAN router that interfaces to a broadband Internet connection. This configuration is similar to one needed for a home or small office. Free access encourages patrons to purchase coffee and other goodies as they surf the web and correspond with e-mail.

In cases where the hotspot owner wants to charge for access, then the wireless LAN system needs to include an access controller and billing function as shown in **Figure 5-7**. When a user runs her web browser, the access controller automatically redirects her to a web page that prompts the user to log in or sign up for service. Billing options include per-minute, per-day, or per-month plans. The billing system keeps track of usage and automatically charges credit cards.

Figure 5-7. Public Wireless LANs Require Components That Fall Outside the Scope of Wireless Networking Technologies

Exhibit 1010
Page 158 of 292



Large hotspots require multiple access points, comparable to an enterprise wireless LAN. Public wireless LANs spanning several locations, however, also requires rather sophisticated access control and billing systems. A large hotel chain, for example, might deploy public wireless LANs at a hundred different locations. Users can subscribe for months of access and be able to use the service from any of the hotels. The access control function in this situation requires a centralized server that maintains authentication, authorization, and accounting (AAA) information.

Wireless LANs in Hotels

To offer wireless coverage for their patrons, hotels have been installing access points in convention centers, ballrooms, meeting rooms, lobbies, swimming pool areas, and guest rooms.
A hotel wireless LAN can enable guests to do all of the following during their stay:

- Browse the Web at the pool or in the fitness center.
- Remotely and securely access their corporate networks from their room.
- Review online schedules and get driving directions.
- Share a high-speed Internet connection with multiple conference participants.

Exhibit 1010
Page 159 of 292

- Remotely print from guest rooms to printers in the business center.
- Conduct video conferences with associates or family members.

The staff and management of hotels can also reap huge benefits from wireless LANs. For example, the deployment of a wireless LAN makes the following tasks much easier and efficient:

- Conduct room inspections to see if everything is in order and no damage was done to the room after guests check out of the hotel. The staff can check the room and send feedback to the main computer through an 802.11-enabled PDA.
- Perform security and safety inspections to make sure doors are locked, fire extinguishers are charged, emergency lights are in working order, and so on. All of the information is updated in real time, saving time and the possibility of error.
- Keep in contact with maintenance workers by using wireless LAN phones. Management can contact maintenance whenever needed, resulting in quicker response times.

Ad Hoc Wireless LANs

An ad hoc wireless LAN, as **Figure 5-8** illustrates, does not utilize access points. Instead, each individual user device communicates directly with another user device. The advantage of this configuration is that users can spontaneously form a wireless LAN quickly. Ad hoc networks are also commonly referred to as peer-to-peer networks.

Exhibit 1010
Page 160 of 292

Figure 5-8. Ad Hoc Wireless LANs Offer Simple Setup and Operation



For example, an ad hoc wireless LAN makes it easy for someone to transfer a large file to an associate in a conference room where an infrastructure wireless LAN is not available. Each user simply configures his radio NIC to operate in **ad hoc mode**, and connections are made automatically. In some cases, the users need to ensure that their IP addresses are set within the same subnet.

Ad hoc mode is also beneficial for supporting emergency services where operations might take place in areas where a wired distribution system for interconnecting access points is not practical. A disaster relief group, for example, can quickly set up network connections among staff working in areas afflicted by hurricanes, floods, and terrorist attacks.

Exhibit 1010
Page 161 of 292

Wireless LAN Technologies

802.11 and HiperLAN/2 are the most common standards for wireless LANs. Examine each of these standards.

802.11

The IEEE 802.11 standard specifies a common medium access control (MAC) and several physical layers for wireless LANs. The initial 802.11 standard became available in 1997, but wireless LANs didn't begin to proliferate on a large scale until 2001, when prices fell dramatically. The IEEE 802.11 working group actively continues to enhance the standard to improve the performance and security of wireless LANs.

note



The 802.11 standard specifies use of an infrared light physical layer; however, no products on the market today comply with this version of the standard.

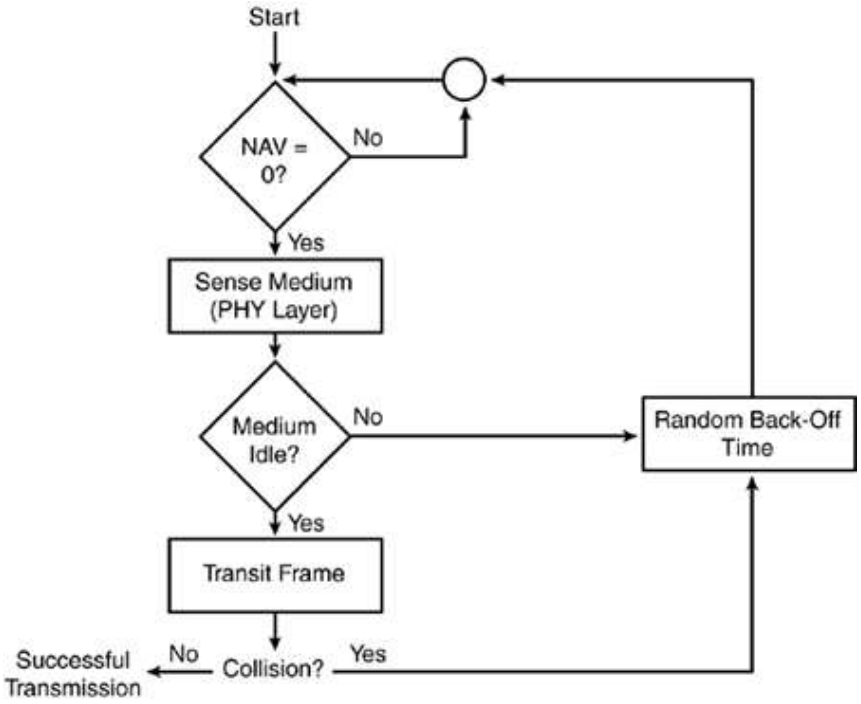
802.11 MAC Layer

The 802.11 standard specifies a single MAC Layer, which provides a variety of functions that support the operation of 802.11-based wireless LANs. The MAC Layer manages and maintains communications between 802.11 stations (radio network cards and access points) by coordinating access to the shared air medium. Often viewed as the brains of the network, the 802.11 MAC Layer directs a particular

802.11 Physical layer, such as 802.11a, 802.11b, or 802.11g, to perform the tasks of sensing the medium, transmission, and receiving of 802.11 frames.

Before transmitting frames, a station must first gain access to the medium, which is a radio channel that stations share. The 802.11 standard defines two forms of medium access: distributed coordination function (DCF) and point coordination function (PCF). DCF is mandatory and based on the CSMA/CA (**carrier sense multiple access** with collision avoidance) protocol. With DCF, 802.11 stations contend for access and attempt to send frames when there is no other station transmitting. (See **Figure 5-9**.) If another station is sending a frame, stations wait until the channel is free.

Figure 5-9. DCF Offers a Distributed Form of Medium Access



As a condition to accessing the medium (see **Figure 5-9**), the MAC Layer checks the value of its network allocation vector (NAV), which is

a counter resident at each station that represents the amount of time that the previous frame needs to be sent. The NAV must be 0 before a station can attempt to send a frame. Prior to transmitting a frame, a station calculates the amount of time necessary to send the frame based on the its length and data rate. The station places a value representing this time in the duration field in the header of the frame. When stations receive the frame, they examine this duration field value and use it as the basis for setting their corresponding NAVs. This process reserves the medium for the sending station.

An important aspect of the DCF is a random back-off timer that a station uses if it detects a busy medium. If the channel is in use, the station must wait a random period of time before attempting to access the medium again. This ensures that multiple stations wanting to send data don't transmit at the same time. The random delay causes stations to wait different periods of time and avoids all of them sensing the medium at exactly the same time, finding the channel idle, transmitting, and colliding with each other. The back-off timer significantly reduces the number of collisions and corresponding retransmissions, especially when the number of active users increases.

With radio-based LANs, a transmitting station can't listen for collisions while sending data, mainly because the station can't have its receiver on while transmitting the frame. As a result, the receiving station needs to send an acknowledgement (ACK) if it detects no errors in the received frame. If the sending station doesn't receive an ACK after a specified period of time, the sending station assumes that there was a collision (or RF interference) and retransmits the frame.

For supporting time-bounded delivery of data frames such as video, the 802.11 standard defines the optional PCF where the access point grants access to an individual station to the medium by polling the station during the contention-free period. Stations can't transmit frames unless the access point polls them first. The period of time for PCF-

Exhibit 1010
Page 164 of 292