vide enhanced security over 2.4-GHz systems because of less range.

In most cases, you'll probably determine that 2.4 GHz is the way to go for common office applications. 2.4-GHz products are certainly inexpensive and capable of supporting most application requirements. Some situations, how ever, benefit from the use of 5 GHz, such as densely populated environments and multimedia applications.

Wi-Fi

The Wi-Fi Alliance, which began its work known as the Wireless Ethernet Compatibility Alliance (WECA), is an international nonprofit organization focusing on the marketing and interoperability of 802.11 wireless LAN products. The Wi-Fi Alliance is the group that pushes the term Wi-Fi to cover all forms of 802.11-based wireless networking, such as 802.11a, 802.11b, 802.11g, or whatever becomes available in the future. Wi-Fi Alliance is also behind **Wi-Fi Protected Access (WPA)**, the stepping stone between the much-criticized WEP and the 802.11i security standard.

The Wi-Fi Alliance has three main goals:

- Promote Wi-Fi certification worldwide by encouraging manufacturers to follow standardized 802.11 processes in the development of wireless LAN products.
- Market Wi-Fi certified products to consumers in the home, small office, and enterprise markets.
- Test and certify Wi-Fi product interoperability.

What Wi-Fi Means

Exhibit 1010
Page 176 of 292

Wi-Fi certification is a process that assures interoperability between 802.11 wireless LAN equipment, including access points and radio cards complying with a variety of form factors. In order to qualify for obtaining Wi-Fi certification for products, a company must become a member of the Wi-Fi Alliance.

The Wi-Fi Alliance follows an established testing program to certify that products are interoperable with other Wi-Fi certified products. After a product successfully passes every test, the manufacturer is granted the right to use the Wi-Fi Certified logo on that particular product and its corresponding packaging and manuals.

Wi-Fi certification is meant to give consumers confidence that they are purchasing wireless LAN products that have met multivendor interoperability requirements. A Wi-Fi logo on the product means that it has met interoperability testing requirements and definitely works with other vendors' Wi-Fi–certified products.

Wi-Fi Protected Access

802.11 WEP doesn't provide enough security for most enterprise wireless LAN applications. Because of static key usage, it's fairly easy to crack WEP with off-the-shelf tools. This motivates IT managers to use stronger and more dynamic forms of WEP.

The problem to date, however, is that these enhanced security mechanisms are proprietary, making it difficult to support multivendor client devices. As a result, the Wi-Fi Alliance took a bold step forward to expedite the availability of effective standardized wireless LAN security by defining WPA while promoting interoperability. With WPA, an environment having many different types of 802.11 radio NICs—such as public hotspots—can benefit from enhanced forms of encryption.

WPA 1.0 is a snapshot of the initial, unratified version of 802.11i, which includes Temporal Key Integrity Protocol (TKIP) and 802.1x

Exhibit 1010
Page 177 of 292

mechanisms. The combination of these two mechanisms provides dynamic key encryption and mutual authentication, something much needed in wireless LANs.

For authentication, WPA 1.0 uses a combination of open system and 802.1x authentication. Initially, the wireless client authenticates with the access points, which authorizes the client to send frames to the access point. Next, WPA performs user-level authentication with 802.1x. During this, WPA 1.0 interfaces to an authentication server in an enterprise environment. WPA 1.0 is also capable of operating in what's known as pre-shared key mode, if no external authentication server is available, such as in homes and small offices.

The 802.11i standard is backward compatible with WPA 1.0; however, 802.11i also includes an optional Advanced Encryption Standard (AES) encryption. AES requires coprocessors not found in most access points today, which makes AES more suitable for new wireless LAN installations. The newer WPA 2.0 includes AES.

HiperLAN/2

HiperLAN/2, which stands for High Performance Radio LAN, is a wireless LAN standard developed by the Broadband Radio Access Networks (BRAN) division of the European Telecommunications Standards Institute (ETSI). HiperLAN/2 defines an efficient, high-speed wireless LAN technology that fully meets the requirements of Europe's spectrum regulations.

HiperLAN/2 has a physical layer that is similar to IEEE's 802.11a, which operates at up to 54 Mbps in the 5-GHz band using OFDM. A major difference with HiperLAN/2 is the use of a connection-oriented protocol with time division multiplexing as the basis for supporting data transfer between users. This method of transmission is efficient for multimedia applications including voice and video.

HiperLAN/2 Enhancements

Exhibit 1010
Page 178 of 292

The similarities between 802.11a and HiperLAN/2, however, stop at the MAC Layer. While 802.11a uses CSMA/CA to transmit packets, HiperLAN/2 uses Time Division Multiple Access (TDMA). A problem is that CSMA/CA causes stations to wait for an indefinite period of time, which is referred to as asynchronous access. With this mode of operation, there are not any regular time relationships associated with medium access. As a result, there's no guarantee of when a particular station will be able to send a packet. The lack of regular access to the medium draws down the efficiency of the system, which is not good for supporting voice and video information.

The use of TDMA in HiperLAN/2, however, offers a regular time relationship for network access. TDMA systems dynamically assign each station a time slot based on the station's need for throughput. The stations then transmit at regular intervals during their respective time slots, making more efficient use of the medium and improving support of voice and video applications.

HiperLAN/2 has a number of attractive features as compared to 802.11. The first, and probably most important, is higher throughput. Both 802.11a and HiperLAN/2 boast maximum data rates of 54 Mbps, but this doesn't represent the actual rate that information flows between the station and the access point.

The true usable maximum throughput of HiperLAN/2 is 42 Mbps, while the maximum usable throughput of 802.11a is only around 18 Mbps. This puts HiperLAN/2 well ahead of 802.11a in terms of performance of each access point.

A unique feature of HiperLAN/2 technology is the ability to interface with other high-speed networks, including 3G cellular, asynchronous transfer mode (ATM), and other Internet protocol-based networks. This can be a real advantage when integrating wireless LANs with cellular systems and WANs.

Exhibit 1010
Page 179 of 292

Is HiperLAN/2 a Threat to 802.11?

Despite bold predictions of mass production and deployment of HiperLAN/2 products during the second half of 2002, not many, if any HiperLAN/2 products are currently available for consumer purchase. In fact, exhaustive searches on the Internet reveal no HiperLAN/2 products available to consumers. HiperLAN/2 doesn't seem to be moving forward at any discernable pace.

Much of this has to do with regulatory issues and big supporters pulling out of the HiperLAN/2 movement. In addition, the 802.11h Task Group has been working on revisions to 802.11 that make it more suitable for deployment in Europe, which is where HiperLAN/2 could dominate if anywhere.

Essentially 802.11h is 802.11a with two additional European features. The first of these is Transmit Power Control (TPC), which enables automatic controls for keeping transmissions from interfering with other nearby systems. The second feature is Dynamic Frequency Selection (DFS), which allows the station to listen to the airspace before picking a channel. This is also an interference avoidance mechanism that the ETSI requires for operation within Europe.

802.11 currently has a definite lead in the worldwide market as the top choice for wireless LAN deployments. This makes 802.11 the only alternative for wireless LAN deployments today. Combined with the absence of HiperLAN/2 products, it's doubtful that HiperLAN/2 will catch up and become the dominant player in the wireless LAN market.

Exhibit 1010
Page 180 of 292

Chapter Summary

Wireless LAN components include radio NICs, access points, routers, repeaters, and antennae that enable wireless applications in buildings and campus areas. These components are building blocks for implementing wireless LANs in homes, small offices, enterprises, and public hotspots. These networks can range from having a single access point in a home or small office to hundreds of access points covering a large facility. Or, the wireless LAN might include only two users communicating directly with each other using ad hoc mode.

802.11 is by far the most prominent standard worldwide, with data rates up to 54 Mbps and operation in either the 2.4-GHz or 5-GHz frequency bands. Wi-Fi offers assurance of interoperability among manufacturers of 802.11-compliant wireless LAN components, and HiperLAN/2 is a European-based standard that is unlikely to compete heavily with 802.11.

Chapter Review Questions

You can find the answers to the following questions in **Appendix A**, "Answers to Chapter Review Questions."

1: Which wireless LAN component is most commonly used in home and small offices?

2: What is the primary difference between an access point and a wireless LAN router?

3: When would the use of a wireless LAN repeater make sense?

4: How does a wireless LAN radio NIC identify with which access point to associate?

5: WEP is a mandatory encryption mechanism. True or false?

6: In what frequency band does 802.11a operate in?

7: How many non-overlapping channels are available with 802.11b wireless LANs?

8: True of false: 802.11g operates at up to 54 Mbps and interoperates with 802.11b.

9: Which 802.11 frequencies are available almost worldwide?

Exhibit 1010
Page 182 of 292

10: What does Wi-Fi provide?

Exhibit 1010
Page 183 of 292

Chapter 6. Wireless MANs: Networks for Connecting Buildings and Remote Areas

What You Will Learn

After reading this chapter, you should be able to

- Recognize specific wireless MAN applications
- **Understand wireless MAN components and technologies**
- **Realize the different types of wireless MAN systems**

Wireless MANs satisfy needs for networking over metropolitan areas, such as cities and specific rural areas. Generally, wireless MANs provide interconnections among stationary users. In most cases, wireless MANs offer stationary outdoor connections.

Wireless MANs offer a high return on investment because companies can avoid leasing or installing expensive copper circuits or optical fiber links. In fact, it's sometimes impossible to install a wired network between two points when right-of-way restrictions prohibit the installation of wires. For example, a company might use wireless MAN components for data communications between the corporate headquarters and a nearby distribution center.

In many cases, companies can realize enough savings from a wireless MAN to pay for the equipment within one to two years. This certainly gives incentive to any company needing to establish communications between buildings spread throughout a metropolitan area.

This chapter offers examples of wireless MAN components, describes how these components interconnect to form a variety of systems, and

explores the various standards.

Exhibit 1010
Page 185 of 292

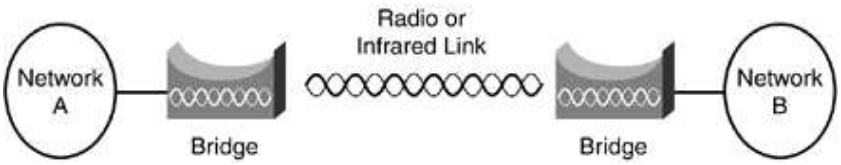
Wireless MAN Components

Components of a wireless MAN generally come in matching pairs because they support fixed wireless connectivity from one point to another. Take a look at the primary components of a wireless MAN.

Bridges

The industry definition of a **bridge** is a device that connects two networks that might use the same or a different data-link layer protocol (Layer 2 of the OSI reference model). **Figure 6-1** illustrates this concept.

Figure 6-1. Bridges Enable the Connection of Two Networks



Wireless bridges are generally at each end of a point-to-point link, such as those that interconnect two buildings. A bridge has a wired port that connects to the network and a wireless port that interfaces with a transceiver. The bridge receives packets on one port and retransmits them on another port. A bridge will not start retransmission until it receives a complete packet. Because of this, stations on either side of a bridge can transmit packets simultaneously without causing collisions.

Exhibit 1010
Page 186 of 292

Some bridges retransmit every packet on the opposite port regardless if the packet is heading to a station located on the opposite network. A learning bridge, which is more common, examines the destination address of every packet to determine whether it should forward the packet based on a decision table that the bridge builds over time. This increases efficiency because the bridge will not retransmit a packet if it knows that the destination address is on the same side of the bridge as the sending address. Learning bridges also age address-table entries by deleting addresses that have been inactive for a specified amount of time.

The bridges within the network are transparent to users. Packets are sent through the bridge automatically. In fact, users have no idea that their packets are traversing a link leading to a different location.

Bridges Versus Access Points

Access points connect multiple users wirelessly to each other and to a wired network. For example, several users equipped with 802.11 NICs might associate with a single access point that connects to an Ethernet network. Each of these users has access to the Ethernet network and to each other. The access point in this case is similar to a bridge device, but the access point interfaces a network to multiple users. A bridge interfaces only other networks.

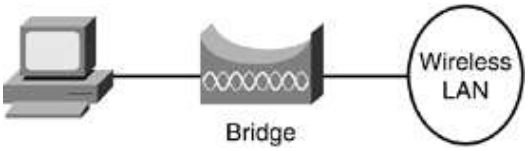
It's possible to use a wireless bridge indoors. For example, a wireless LAN bridge can interface an Ethernet network directly to a particular access point. This might be necessary if few devices, possibly in a far-reaching part of the facility, are interconnected through Ethernet. A wireless LAN bridge plugs into this Ethernet network and uses the 802.11 protocol to communicate with an access point that is within range. In this manner, a bridge enables the wireless connection of a cluster of users (actually a network) to an access point.

Basic Ethernet-to-Wireless Bridges

Exhibit 1010
Page 187 of 292

An Ethernet-to-wireless bridge (see **Figure 6-2**) connects directly to a single computing device through an Ethernet port and then provides a wireless connection to an access point. This makes it useful when the device, such as a printer, PC, or video game console, has an Ethernet port and no wireless NIC. In some cases, you might have no way of adding a wireless NIC, which makes a basic bridge the only way to go wireless. Printers and video game machines are common examples of this scenario.

Figure 6-2. Basic Bridge Connects a PC to a Wireless LAN



Workgroup Bridges

Workgroup bridges are the answer for connecting wireless networks to larger, wired Ethernet networks. A workgroup bridge acts as a wireless client on the wireless network, and then interfaces to a wired network. The wired side connects to an Ethernet switch that connects multiple devices. A workgroup bridge offers more robust and higher-end management and security utilities—with higher prices—as compared to a basic bridge.

Figure 6-3. Workgroup Bridge Connects to Standard Wired Networks

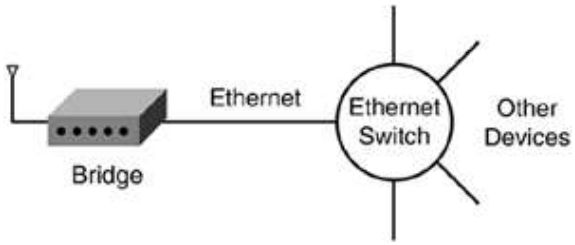
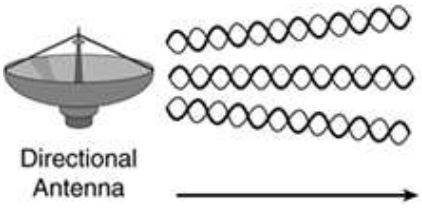


Exhibit 1010
Page 188 of 292

Directional Antennae

The antenna is an important element of a wireless MAN. Unlike other types of wireless networks, most antennae for wireless MANs use directional antennae, mainly because they operate over wider areas. Figure 6-4 illustrates the propagation of radio waves from a directional antenna. This contrasts with an omnidirectional antenna, which transmits radio waves in all directions.

Figure 6-4. Directional Antennae Maximize the Intensity of Radio Waves in One Direction



Different types of antennae have different vertical and horizontal beamwidths. For example, an omnidirectional antenna has a horizontal beamwidth of 360 degrees and a vertical beamwidth that ranges from 7 to 80 degrees. A semidirectional antenna might have a vertical beamwidth of 20 degrees and a horizontal beamwidth of 50 degrees. Generally, the narrower the beamwidth, the longer the range when transmit power is kept constant.

Semidirectional Antennae

There are several different types of antennae that have semidirectional radiation patterns. For example, a directional patch antenna will have at least double the range as compared to an omnidirectional antenna. You can easily mount a patch antenna on a wall on one side of a facility and effectively cover a large area. A Yagi antenna, a com-

mon antenna invented by Japanese inventor Hidetsugu Yagi, is the semidirectional antenna best for long-range applications.

Semidirectional antennae effectively increase the signal's amplitude—referred to as gain—by approximately 10 times. Their use is mostly for extending wireless LANs to cover a larger area. For example, a university might employ a Yagi antenna to effectively cover a large, open, outdoor area of the campus. Wireless MANs generally span much greater distances and require greater values of gain.

Highly Directional Antennae

A highly directional antenna has an extremely narrow beamwidth, with long radiation patterns and corresponding range. To achieve this degree of directivity, you need to use dish antennae that focus the radio energy mostly in one direction. These types of antennae are expensive compared to omni- and semidirectional antennae; however, the costs may be feasible if the solution requires long range.

Many of the higher-gain directional antennae use a parabolic dish to focus the radio frequency (RF) power in one direction. A parabolic dish, for example, has a narrower horizontal and vertical beamwidth of 4 to 25 degrees. This extreme focusing of the RF power increases range significantly.

A problem, however, is that the dish antennae are subject to damage from weather because of excessive wind loading, especially if the antenna is not mounted correctly. As a result, highly directional grids that have plenty of holes in the dish are generally safer to deploy.

In addition, both semidirectional and highly directional antennae require a clear line of sight between both ends of the system. In some cases, RF signals can pass through trees and some buildings, but infrared requires an unobstructed path. RF and infrared signals also experience periodic attenuation due to obstructions moving across the path of the signal, such as passing trains and automobiles. Planning

Exhibit 1010
Page 190 of 292

wireless MANs is difficult in city environments because of buildings that block the path between the ends of the system.

Effect of Polarization

Antenna polarization is the physical orientation of the antenna along a horizontal or vertical plane. For example, vertical polarization, which is the most common for wireless LANs, occurs when the antenna is perpendicular to the Earth. Parallel polarization applies to an antenna that is parallel to the Earth.

To maximize the transfer of RF energy from the transmitter to the receiver antenna, both antennae should have the same polarization. If one antenna has vertical polarization and the other has horizontal polarization, no transfer of power or communications will occur.

Exhibit 1010
Page 191 of 292