- 802.15.4— This group, Task Group 4, is investigating the definition of a standard with low data rates that leads to extremely low-power consumption for small devices where it's not practical to change batteries within months or years. For example, sensors, smart badges, and home automation systems are candidates for this technology. Data rates include 20, 40, and 250 kbps. A draft of the 802.15.4 standard is now available for purchase.

note



For more information and updates regarding the 802.15 standard, refer to http://grouper.ieee.org/groups/802/15/.

Bluetooth

The introduction of Bluetooth in 1998 was the result of several companies, including Ericsson, IBM, Intel, Nokia, and Toshiba, working together to create a solution for wireless access among computing devices. Bluetooth, which is a specification and not a standard, is ideal for small devices with short-range, low-power, and inexpensive radio links. This makes Bluetooth a good solution for connecting small devices within range of a person in a small working area. That's why the 802.15 chose Bluetooth as the basis of the 802.15.1 standard.

Basic Features

The Bluetooth Special Interest Group (SIG) published the initial version of the specification in mid-1999. There have been updates since then, but the technical attributes are essentially the same. Bluetooth transceivers operate at up to 1 Mbps data rate in the 2.4GHz band, using FHSS technology. It constantly hops over the entire spectrum at a rate of 1,600 hops per second, which is much faster than the 802.11 version of frequency hopping.

Exhibit 1010
Page 135 of 292

Low-power Bluetooth devices have a range of 30 feet. High-power Bluetooth devices, however, can reach distances of around 300 feet. The high-power mode, though, is rare.

Bluetooth modules have relatively small form factors. Typical measurements are 10.2 × 14 × 1.6 millimeters, which is small enough to fit in a variety of user devices.

Bluetooth enables automatic connection among Bluetooth devices that fall within range of each other, but a user has the ability to accept and disallow connections with specific users. Users, however, should always be aware of whether their Bluetooth connection is enabled. To ensure security, disable the Bluetooth connection. Encryption is also part of the specification.

Could Bluetooth Replace Wireless LANs?

Bluetooth has characteristics similar to wireless LANs. Through the use of the high-power version of Bluetooth, manufacturers can develop Bluetooth access points and routers with a similar range as 802.11 networks. The current Bluetooth products, however, are mostly low power and focus on wireless PAN functions. In addition, it would be difficult for any Bluetooth wireless LAN products to gain a strong foothold in the market because 802.11 products already have widespread adoption.

The place where Bluetooth falls behind 802.11 is performance and range. 802.11 components can reach data rates of up to 54 Mbps, while Bluetooth lags way behind at around 1 Mbps. This might be good enough for most cable replacement applications— such as an interface between headphones and a PDA— but higher performance is necessary when surfing the web through a broadband connection or participating on a corporate network. Also, the range of 802.11 is typically 300 feet inside offices, which is much greater than Bluetooth.

Exhibit 1010
Page 136 of 292

Bluetooth would require many access points to fully cover larger areas.

As a result, it's highly unlikely that Bluetooth products will win over 802.11. This is certainly apparent because electronics stores primarily sell 802.11 (Wi-Fi) solutions for wireless LAN applications, not Bluetooth.

Could Wireless LANs Replace Bluetooth?

It's possible that 802.11 wireless LANs could have a big impact on the sale of Bluetooth devices, mostly because 802.11 meets or exceeds nearly all of the characteristics of Bluetooth. Because widespread adoption of Bluetooth is still lacking, there's time for 802.11 vendors to get their foot in the door with manufacturers needing support for wireless PANs.

Some modifications would need to be made, however. The size of 802.11 components needs to be smaller, but that is becoming more of a reality as semiconductor companies strive for miniaturization of their 802.11 chipsets. These smaller components require less power, making them more competitive for devices, such as mobile phones, that have smaller batteries. With the 802.15 group defining standards for wireless PANs based on Bluetooth— and the 802.11 group focusing on wireless LANs— it's likely that both Bluetooth and 802.11 will continue to coexist and complement each other.

Minimizing Bluetooth Interference

As more wireless products become available, you need to carefully manage potential frequency interference. Tests have shown significant interference between Bluetooth and other systems operating in the 2.4 GHz band, such as 802.11 wireless LANs. A critical problem is that Bluetooth and 802.11b neither understand each other nor follow the same rules. A Bluetooth radio might haphazardly begin transmitting data while an 802.11 station is sending a frame. This results in a

Exhibit 1010
Page 137 of 292

collision, which forces the 802.11 station to retransmit the frame. This lack of coordination is the basis for radio frequency (RF) interference between Bluetooth and 802.11.

Because of the potential for collisions, 802.11 and Bluetooth networks suffer from lower performance. An 802.11 station automatically lowers its data rate and retransmits a frame when collisions occur. Consequently, the 802.11 protocol introduces delays in the presence of Bluetooth interference.

The full impact of RF interference depends on the utilization and proximity of Bluetooth devices. Interference occurs only when both Bluetooth and 802.11b devices transmit at the same time. Users might have Bluetooth devices in their PDAs or laptops, but no interference will exist if their applications are not using the Bluetooth radio to send data.

Some Bluetooth applications, such as printing from a laptop or synchronizing a PDA to a desktop, utilize the radio for a short period of time. In this case, the Bluetooth devices are not active long enough to noticeably degrade the performance of an 802.11 network. For example, a user might synchronize her PDA to her desktop when arriving at work in the morning. Other than that, their Bluetooth radio might be inactive and not cause interference the rest of the day.

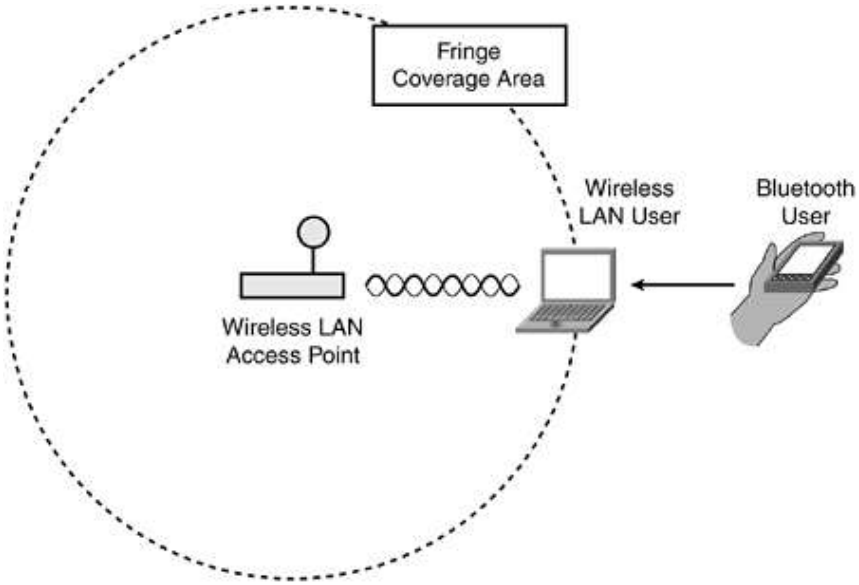
The biggest impact is when a company implements a large-scale Bluetooth network, such as one that enables mobility for doctors and nurses using PDAs throughout a hospital. If the Bluetooth network is widespread and under moderate-to-high levels of utilization, the Bluetooth system will probably offer a substantial number of collisions with an 802.11 network residing in the same area. In this case, Bluetooth and 802.11 would have difficulties coexisting, and performance would likely suffer.

Exhibit 1010
Page 138 of 292

In addition to utilization, the proximity of the Bluetooth devices to 802.11 radio NICs and access points has a tremendous affect on the degree of interference. The transmit power of Bluetooth devices is generally lower than 802.11 wireless LANs. Therefore, an 802.11 station must be relatively close (within 10 feet or so) of a transmitting Bluetooth device before significant interference can occur.

A typical application fitting this scenario is a laptop user utilizing Bluetooth to support connections to a PDA and printer and 802.11 to access the Internet and corporate servers. The potential for interference in this situation is enormous, especially when the user is operating within outer limits of the coverage area of the 802.11 network. Figure 4-7 illustrates this situation. The signal from the Bluetooth device will likely drown out the weaker 802.11 signal because of the distance of the access point.

Figure 4-7. RF Interference Can Occur Between Bluetooth and 802.11 Wireless LAN Devices



Here are some tips on how to avoid interference from Bluetooth devices:

Exhibit 1010
Page 139 of 292

- Manage the use of RF devices— One way to reduce the potential for interference is to regulate the types of RF devices within your home or office. In other words, establish your own private regulatory body for managing unlicensed RF devices. The extreme measure would be to completely ban the use of Bluetooth; however, that is not practical or even possible in all cases. For example, you can't feasibly prohibit the use of Bluetooth in public areas of large offices. For private applications, you could set company policies to limit the use of Bluetooth to specific applications, such as synchronizing PDAs to desktops.
- Ensure adequate 802.11 coverage— Strong, healthy 802.11 signals throughout the coverage areas reduce the impact of the Bluetooth signals. If wireless LAN transmissions become too weak, the interfering Bluetooth signals will be more troublesome. Perform a thorough RF site survey, and determine the appropriate location for access points.
- Move to the 5 GHz band— If none of the preceding steps solve the problem, consider using a 5 GHz wireless LAN such as 802.11a. You can completely avoid RF interference in this band— at least for the foreseeable future.

note



For more information about the Bluetooth specification and related products, refer to **http://www.bluetooth.com**.

IrDA

Bluetooth's primary competitor is Infrared Data Association (IrDA), which has been defining and publishing since 1993. The IrDA has a charter to create an interoperable, low-cost, low-power, serial data communications standard for short-range applications. IrDA has been

Exhibit 1010
Page 140 of 292

around for much longer than Bluetooth. In fact, many laptops and cell phones have been coming equipped with an IrDA interface for years.

Basic Features

The basis for IrDA is infrared light, which doesn't go through walls and other obstacles. This strictly limits the range of IrDA devices to within an obstacle-free room. This makes IrDA useful only for point-to-point applications, such as synchronizing PDAs to PCs. An advantage of IrDA, however, is that there's no worry about RF interference.

The IrDA data standard, which is best for devices such as an MP3 player needing to stream information, offers up to 4 Mbps data rates. This version of the standard has up to 3 feet (1 meter range), but low-power versions significantly conserve battery power and reduce operation to approximately 8 inches (20 centimeters).

To effectively support wireless computer peripherals, such as a keyboard or mouse, the IrDA control version of the standard reduces data rates to 75 kbps. In addition, the host computer can communicate with up to eight peripherals simultaneously.

note



For more information regarding the IrDA specification and related products, refer to **http://www.irda.org**.

Exhibit 1010
Page 141 of 292

Chapter Summary

Wireless PANs are meant to provide wireless network connections in small areas, such as within a room. Devices equipped with Bluetooth or IrDA significantly reduce cables, which increases the flexibility of applications— such as hands-free operation of cell phones, listening to streaming audio players, and synchronizing a PDA to a computer. Many of the types of applications fall within both home and enterprise.

Bluetooth and IrDA are the primary technologies that wireless PANs implement. The 802.15 group elected the use of Bluetooth as the basis for the 802.15.1 standard for wireless PANs. Because of limited range and performance of Bluetooth, it's not likely that wireless PANs will replace 802.11 wireless LANs.

Exhibit 1010
Page 142 of 292

Chapter Review Questions

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

1: What form factors are common for wireless PAN radio cards?

2: What application can strongly benefit through the use of a wireless USB adapter (also referred to as a wireless dongle)?

3: When would the use of a wireless PAN router make sense?

4: What is the general maximum coverage area of a wireless PAN?

5: Which IEEE standards group uses Bluetooth as the basis for the standard?

6: In what frequency band does Bluetooth operate?

7: What is the primary issue of using Bluetooth around 802.11 wireless LANs?

8: A Bluetooth-enabled device is always transmitting. True or false?

9: What is the highest possible data rate of an IrDA device?

Exhibit 1010
Page 143 of 292

10: What is a benefit of IrDA as compared to Bluetooth?

Exhibit 1010
Page 144 of 292

Chapter 5. Wireless LANs: Networks for Buildings and Campuses

What You Will Learn

After reading this chapter, you should be able to

- Recognize specific wireless LAN applications
- **Understand wireless LAN components and standards**
- **Understand the configuration of wireless LAN systems**

Wireless LANs effectively satisfy needs within buildings and campus environments. With performance and security comparable to wired networks, wireless LAN solutions are found in homes, small offices, enterprises, and public areas. Wireless LANs are able to support many different types of applications.

This chapter defines each of the primary wireless LAN components, describes how these components interconnect to form a variety of systems, and explores the 802.11 standards.

Exhibit 1010
Page 145 of 292

Wireless LAN Components

Wireless LANs consist of components similar to traditional Ethernet-wired LANs. In fact, wireless LAN protocols are similar to Ethernet and comply with the same form factors. The big difference, however, is that wireless LANs don't require wires.

User Devices

Users of wireless LANs operate a multitude of devices, such as PCs, laptops, and PDAs. The use of wireless LANs to network stationary PCs is beneficial because of limited needs for wiring. Laptops and PDAs, however, are commonly equipped with wireless LAN connectivity because of their portable nature. User devices might consist of specialized hardware as well. For example, bar code scanners and patient monitoring devices often have wireless LAN connectivity.

Radio NICs

A major part of a wireless LAN includes a radio NIC that operates within the computer device and provides wireless connectivity. A wireless LAN radio NIC, sometimes referred to as a radio card, often implements the 802.11 standard. The cards generally implement one particular physical layer, such as 802.11a or 802.11b/g. As a result, the radio card must utilize a version of the standard that is compatible with the wireless LAN. Wireless LAN radio cards that implement multiple versions of the standard and provide better **interoperability** are becoming more common.

Radio cards come in a variety of form factors, including: ISA, PCI, PC card, mini-PCI, and CF. PCs generally utilize ISA and PCI cards; but

PDAs and laptops use PC cards, mini-PCI, and CF adapters.

Access Points

An access point contains a radio card that communicates with individual user devices on the wireless LAN, as well as a wired NIC that interfaces to a **distribution system**, such as Ethernet. System software within the access point bridges together the wireless LAN and distribution sides of the access point. The system software differentiates access points by providing varying degrees of management, installation, and security functions. **Figure 5-1** shows an example of access-point hardware.

Figure 5-1. Wireless LAN Access Points Connect Wireless LANs to Wired Networks (Photo Courtesy of Linksys)



In most cases, the access point provides an http interface that enables configuration changes to the access point through an end-user device that is equipped with a network interface and a web browser. Some access points also have a serial RS-232 interface for configuring the access point through a serial cable as well as a user device running terminal emulation and Telnet software, such as hyper terminal.

Configuring an Access Point

Exhibit 1010
Page 147 of 292

Look at the basic radio configuration settings for a Cisco 350 access point. These types of settings are common for other access points as well.

One parameter that you should set is the service set identifier (SSID). The SSID provides a name for the specific wireless LAN that users will associate with. For security purposes, it's a good idea to set the SSID to something other than the default value.

For most applications, set the transmit power of the access point to the highest value, which is typically 100 milliwatt (mW) in the United States. This will maximize the range of the wireless LAN. The actual maximum effective power output is 1 watt, but the lower transmit power allows enough margin to allow the use of a higher-gain antenna and still remain within limitations.

In the United States, set the access point to operate on any one of the channels in the range from 1 through 11. When installing only one access point, it doesn't matter which channel you choose. If you install multiple access points, or you know of a nearby wireless LAN within range of yours, you need to select different non-overlapping channels (such as channels 1, 6, and 11) for each access point within range of one another.

As a minimum, activate wired equivalent privacy (WEP) encryption as a minimum level of security. You'll need to assign an encryption key that all user devices will need in order to interface with the access point with encrypted data. If you choose to implement 40-bit keys, enter 10 hexadecimal characters, with each character having the value of 1 through 9 or A through F. The 104-bit keys require 26 hexadecimal characters. Keep in mind that 40-bit keys correspond with 64-bit encryption and 104-bit keys correspond with 128-bit encryption to the addition of a 24-bit initialization vector in both cases.

Exhibit 1010
Page 148 of 292

Routers

By definition, a router transfers packets between networks. The router chooses the next best link to send packets on to get closer to the destination. Routers use Internet Protocol (IP) packet headers and routing tables, as well as internal protocols, to determine the best path for each packet.

A wireless LAN router adds a built-in access point function to a multiport Ethernet router. This combines multiple Ethernet networks with wireless connections. A typical wireless LAN router includes four Ethernet ports, an 802.11 access point, and sometimes a parallel port so it can be a print server. This gives wireless users the same ability as wired users to send and receive packets over multiple networks.

Routers implement the Network Address Translation (NAT) protocol that enables multiple network devices to share a single **IP address** provided by an Internet service provider (ISP). **Figure 5-2** illustrates this concept. Routers also implement Dynamic Host Configuration Protocol (DHCP) services for all devices. DHCP assigns private IP addresses to devices. Together, NAT and DHCP make it possible for several network devices, such as PCs, laptops, and printers to share a common Internet IP address.

Figure 5-2. NAT and DHCP Are Essential Protocols That Routers Implement

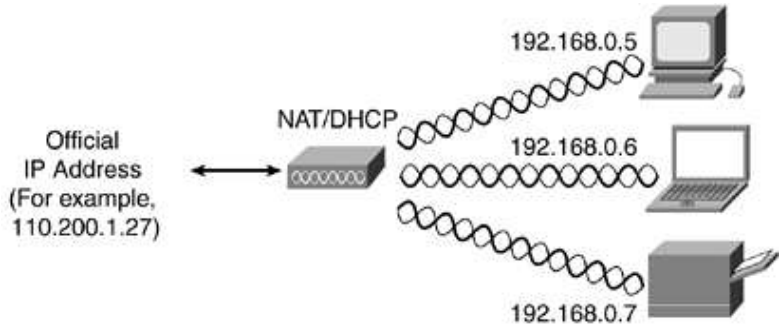


Exhibit 1010
Page 149 of 292