WiFi for the Enterprise

Nathan J. Muller

McGraw-Hill
New York Chicago San Francisco Lisbon
London Madrid Mexico City Milan New Delhi
San Juan Seoul Singapore Sydney Toronto

The McGraw-Hill Companies

Cataloging-in-Publication Data is on file with the Library of Congress.

1 2 3 4 5 6 7 8 9 0 DOC/DOC 0 9 8 7 6 5 4 3

ISBN 0-07-141252-2

The sponsoring editor for this book was Steve Chapman and the production supervisor was Pamela A. Pelton. It was set in Century Schoolbook by MacAllister Publishing Services, LLC.

Printed and bound by RR Donnelley.

This book is printed on recycled, acid-free paper containing a minimum of 50 percent recycled de-inked fiber.

McGraw-Hill books are available at special quantity discounts to use as premiums and sales promotions, or for use in corporate training programs. For more information, please write to the Director of Special Sales, Professional Publishing, McGraw-Hill, Two Penn Plaza, New York, NY 10121-2298. Or contact your local bookstore.

CHAPTER 1

WiFi in Perspective

Of all the communications services available today, wireless services are having the most dramatic impact on our personal and professional lives, enhancing personal productivity, mobility, and security. In particular, the impact of cellular phone services on our lives is well documented, but *Wireless Fidelity* (WiFi) also promises to have a dramatic effect in the near future. In fact, emerging broadband cellular phone and WiFi services are not mutually exclusive, but complementary, so much so that a single PC Card for notebooks and some *personal digital assistants* (PDAs) will soon support both services, switching between the two networks automatically as the user changes locations or applications.

WiFi operates in unlicensed frequency bands and is based on a set of standards promulgated by the *Institute of Electrical and Electronics Engineers* (IEEE). One standard, called 802.11b, specifies the requirements for connecting devices at the maximum throughput rate of 11 Mbps using the 2.4 GHz frequency band, whereas 802.11a specifies the requirements for connecting devices at the maximum throughput rate of 54 Mbps using the 5 GHz frequency band. Proprietary extensions to each of these standards enable speed bursts of 22 Mbps and 72 Mbps, respectively.

As the cost of wireless equipment continually decreases to the point of reaching parity with wired gear, WiFi networks are now being used in a number of settings, such as college campuses, business parks, office buildings, and even homes. Such networks are also being implemented by a number of service providers in public places such as airports, hotels, retail locations, and cafes to give users of notebook computers and handheld devices wireless access to the Internet for e-mail and web browsing. In the corporate environment, WiFi enables users to access *local area networks* (LANs) to search databases, share files, and print documents—all without requiring them to find an available port and set up a cable connection. And since many employees visit other locations in a building or campus throughout the day, wireless connections facilitate mobility without impeding productivity.

Aside from the low cost of equipment, the growing popularity of WiFi networks has occurred for several other reasons:

- They not only work, but they work well, and they are undergoing continuous refinement, particularly in the area of security.
- Wireless connections are easy to set up, especially with Windows XP, which provides integral support for WiFi, eliminating the need to manually install drivers. Some notebook computers even come with WiFi antennas embedded into their lids, eliminating the need for a PC Card for *wireless LAN* (WLAN) connections.

- There is nothing new to learn about using WiFi; anyone who uses an Ethernet LAN at work or home will readily appreciate the convenience and performance of WiFi, which is also based on Ethernet.
- Connectivity is available from a growing number of service providers, so WiFi can be used between the home and workplace at various *hot spots* such as airports, hotels, and cafes, which greatly extends its utility.

Many other wireless technologies are available. To put WiFi into the proper context, it is helpful to survey some of the other wireless alternatives available to businesses and telecommuters, and examine the applications for which they are best suited. Sometimes WiFi will complement another wireless technology such as Bluetooth or *General Packet Radio Service* (GPRS), enabling the user to benefit from having access to both, depending on the location or type of application.

Bluetooth

Bluetooth is an omnidirectional wireless technology that provides limited range voice and data transmission over the same unlicensed 2.4 GHz frequency band used by WiFi, allowing connections with a wide variety of fixed and portable devices that normally would have to be cabled together. Up to eight devices—one master and seven slaves—can communicate with one another in a so-called piconet at distances of up to 30 feet. Table 1-1 summarizes the performance characteristics of Bluetooth.

Applications

Among other things, users can swap data and synchronize files using Bluetooth merely by having the devices come within range of one another. Images captured with a digital camera, for example, can be dropped off at a PC for editing or a color printer for output on photo-quality paper—all without having to connect cables, load files, open applications, or click buttons.

The technology is a combination of circuit switching and packet switching, making it suitable for voice as well as data. Instead of fumbling with a cell phone while driving, for example, a user can wear a lightweight headset to answer a call and engage in a conversation even if the phone is tucked away in a briefcase or purse.

Table 1-1

Performance characteristics of Bluetooth

Feature/Function	Performance
Frequency band	2.4 GHz *Industrial, Scientific, and Medical* (ISM) band.
Connection type	*Frequency-hopping spread spectrum* (FHSS).
Hop rate	1,600 hops per second among 79 frequencies.
Transmission power	1 *milliwatt* (mW).
Aggregate data rate	1 Mbps using frequency hopping.
Range	Up to 30 feet (9 meters).
Supported stations	Up to 8 devices per piconet.
Voice channels	Up to 3 synchronous channels.
Data security	For authentication, a 128-bit key is used; for encryption, the key size is configurable between 8 and 128 bits.
Addressing	Each device has a 48-bit *Media Access Control* (MAC) address that is used to establish a connection with another device.

Although WLANs are useful in minimizing the need for cables, they are not normally used for interconnecting the range of mobile devices people carry around everyday between home and the office, such as smartphones, PDAs, MP3 players, and digital cameras. For this, Bluetooth is needed. In the office, a Bluetooth portable device can be in motion while connected to the LAN *access point* (AP) as long as the user stays within the 30-foot range.

Bluetooth can be combined with other technologies to offer wholly new capabilities, such as automatically lowering the ring volume of a cell phone or shutting it off as a user enters quiet zones like churches, restaurants, theaters, and classrooms. Upon leaving the quiet zone, the cell phone is returned to the original settings.

Topology

Bluetooth devices within a piconet play one of two roles: master or slave. The master is the device in a piconet whose clock and hopping sequence is used to synchronize all other devices (slaves) in the piconet. The unit that

carries out the paging procedure and establishes a connection is the master of the connection by default. The slaves are the units within a piconet that are synchronized to the master via its clock and hopping sequence.

The Bluetooth topology is best described as a multiple piconet structure. Because Bluetooth supports both point-to-point and point-to-multipoint connections, several piconets can be established and linked together in a topology called a *scatternet* whenever the need arises (see Figure 1-1).

Piconets are uncoordinated, with frequency hopping occurring independently. Several piconets can be established and linked together ad hoc, where each piconet is identified by a different frequency-hopping sequence. All users participating on the same piconet are synchronized to this hopping sequence. Although the synchronization of different piconets is not permitted in the unlicensed ISM band, Bluetooth units may participate in different piconets through *time division multiplexing* (TDM). This enables a unit to sequentially participate in different piconets by being active in only one piconet at a time.

With its service discovery protocol, Bluetooth enables a much broader vision of networking, including the creation of *personal area networks* (PANs), where all the devices in a person's life can communicate and work together. Technical safeguards ensure that a cluster of Bluetooth devices in public places, such as an airport lounge or train terminal, would not suddenly start talking to one another.

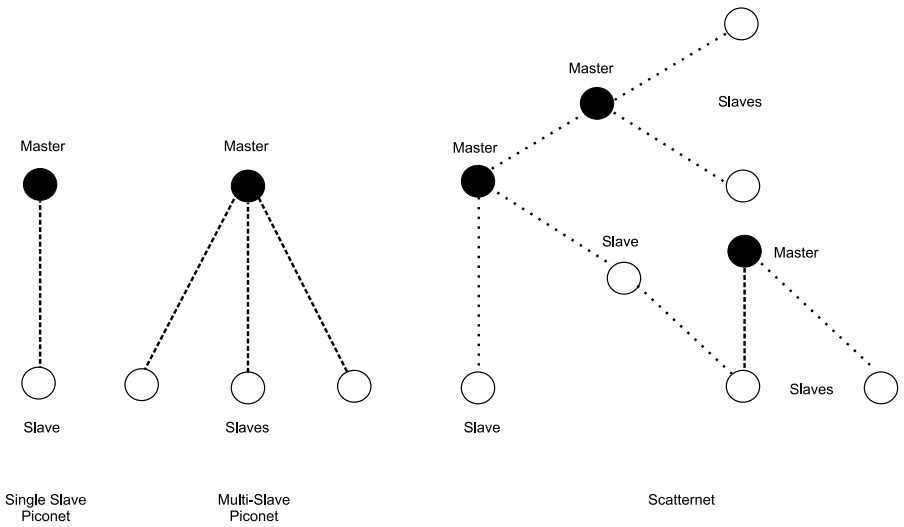

Figure 1-1
The possible topologies of networked Bluetooth devices, where each is either a master or slave

Technology

Two types of links have been defined for Bluetooth in support of voice and data applications: an *asynchronous connectionless* (ACL) link and a *synchronous connection-oriented* (SCO) link. ACL links support data traffic on a best-effort basis. The information carried can be user data or control data. SCO links support real-time voice and multimedia traffic using reserved bandwidth. Both data and voice are carried in the form of packets, and Bluetooth devices can support active ACL and SCO links at the same time.

ACL links support symmetrical/asymmetrical, packet-switched, point-to-multipoint connections that are typically used for data. For symmetrical connections, the maximum data rate is 433.9 Kbps in both directions—send and receive. For asymmetrical connections, the maximum data rate is 723.2 Kbps in one direction and 57.6 Kbps in the reverse direction. If errors are detected at the receiving device, a notification is sent in the header of the return packet, indicating that only lost or corrupt packets need to be retransmitted.

SCO links provide symmetrical, circuit-switched, point-to-point connections that are typically used for voice. Three synchronous channels of 64 Kbps each are available for voice. The channels are derived through the use of either *pulse code modulation* (PCM) or *continuous variable slope delta* (CVSD) modulation. PCM is the standard for encoding speech in analog form into the digital format of ones and zeros. CVSD is another standard for analog-to-digital encoding, but offers more immunity to interference and therefore is better suited than PCM for voice communication over a wireless link. Bluetooth supports both PCM and CVSD; the appropriate voice-coding scheme is selected after negotiation between the link managers of each Bluetooth device before the call takes place.

Voice and data are sent as packets. Communication is handled with *time division duplexing* (TDD), which divides the channel into time slots, each 625 *microseconds* (μs) in length. The time slots are numbered according to the clock of the piconet master. In the time slots, master and slave can transmit packets. In the TDD scheme, master and slave alternatively transmit (see Figure 1-2). The master starts its transmission in even-numbered time slots only, and the slave starts its transmission in odd-numbered time slots only. The start of the packet is aligned with the slot start. Packets transmitted by the master or slave may extend over as many as five time slots.

With TDD, bandwidth can be allocated on an as-needed basis, changing the makeup of the traffic flow as demand warrants. For example, if the user wants to download a large data file, the amount of bandwidth that is

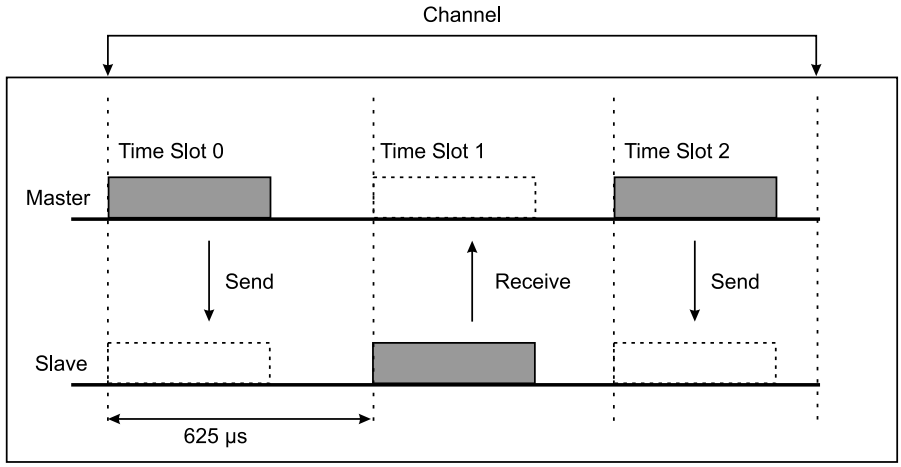

Figure 1-2
With the TDD scheme used in Bluetooth, packets are sent over time slots of 625 μs in length between the master and slave units within a piconet.

needed will be allocated to the transfer. Then, at the next moment, if a file is being uploaded, that same amount of bandwidth can be allocated to that transfer.

Regardless of the application—voice or data—making connections between Bluetooth devices is as easy as powering them up. In fact, one advantage of Bluetooth is that it does not need to be set up—it is always on, running in the background and looking for other devices it can communicate with. When Bluetooth devices come within range of one another, they engage in a service discovery procedure, which entails the exchange of messages to become aware of each other's service and feature capabilities. Having located available services within the vicinity, the user may select from any of them. After that, a connection between two or more Bluetooth devices can be established.

The radio link itself is very robust, using FHSS technology to overcome interference and fading. Spread spectrum is a digital coding technique in which the signal is taken apart, or spread, so that it sounds more like noise as it is sent through the air. The addition of frequency hopping—having the signals skip from one frequency to another—makes wireless transmissions even more secure. Bluetooth specifies a rate of 1,600 hops per second among 79 frequencies. Because only the sender and receiver know the hopping sequence for coding and decoding the signal, eavesdropping is virtually impossible. For enhanced security, Bluetooth also supports device authentication and encryption.

Other frequency-hopping transmitters in the vicinity will use different hopping patterns and much slower hop rates than Bluetooth devices.

Although Bluetooth signals constantly hop over a range of frequencies to avoid interference, WiFi employs *direct sequence spread spectrum* (DSSS), which exposes its signal to interference. Bluetooth and WiFi would not be able to operate together in the same vicinity.

Nevertheless, notebook users can avail themselves of either Bluetooth or WiFi as the application may warrant. It is just a matter of swapping PC Cards to take advantage of the appropriate wireless link, which will establish itself automatically (see Figure 1-3). Although Windows XP now provides integral support for WiFi, the first release of XP did not provide integral support for Bluetooth. At the time of its release, Microsoft did not have a sufficient array of production-quality Bluetooth devices to test. However, Microsoft has since added support for Bluetooth via the Windows XP Service Pack 1, which is available for free download over the Internet.

Some manufacturers already offer notebook computers for the corporate market that have both Bluetooth and WiFi antennas embedded into their lids. The Tecra 9100 from Toshiba Computer Systems Group, for example, integrally supports Bluetooth and WiFi, enabling the user to save the vacant PC Card slot for other purposes. With 2.5G cellular services becoming widely available, offering up to 144 Kbps for data applications, the slot could be used for a GPRS card. All this, plus the notebook's standard *infrared* (IR) port, turns the computer into a quad-mode wireless device.

Figure 1-3 3Com's Wireless Bluetooth PC Card fits into a notebook's PC Card slot, letting the user communicate with other Bluetooth products, including PDAs, printers, digital cameras, and other enabled computers.

Infrared

In addition to its use as a wireless interface to connect notebooks and other portable devices to the desktop computer, infrared technology can be used to implement WLANs over the wavelength band between 780 and 950 *nanometers* (nm). Two categories of infrared systems are commonly used for WLANs. One is *directed infrared*, which uses a very narrow laser beam to transmit data over one to three miles. This approach can be used to connect LANs in different buildings.

The other category is *nondirected infrared*, which uses a less focused approach. Instead of using a narrow beam to convey the signal, the light energy is spread out and bounced off narrowly defined target areas or larger surfaces such as office walls and ceilings. Nondirected infrared links may be further categorized as either line of sight or diffuse (see Figure 1-4). Line-of-sight links require a clear path between the transmitter and receiver, but generally offer higher performance.

The line-of-sight limitation may be overcome by incorporating a recovery mechanism in the infrared LAN, which is managed and implemented by a separate device called a *multiple access unit* (MAU) to which each workstation is connected. When a line-of-sight signal between two stations is temporarily blocked, the MAU's internal optical link control circuitry automatically changes the link's path to get around the obstruction. When the original path is cleared, the MAU restores the link over that path. No data is lost during this recovery process.

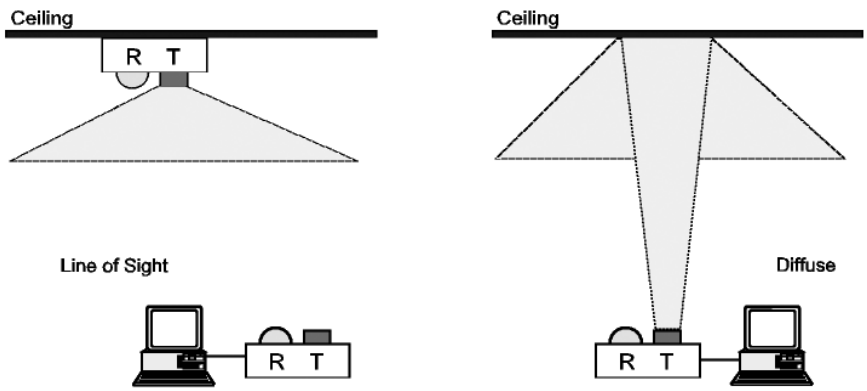

Figure 1-4
Line-of-sight versus diffuse configurations for infrared links

Diffuse links rely on light bounced off reflective surfaces. Because it is difficult to block all of the light reflected from large surface areas, diffuse links are generally more robust than line-of-sight links. The disadvantage of diffused infrared is that a great deal of energy is lost, and, consequently, the data rates and operating distances are much lower.

System Components

Light-emitting diodes (LEDs) or *laser diodes* (LDs) are used for transmitters. LEDs are less efficient than LDs. They typically exhibit only 10 to 20 percent electro-optical power conversion efficiency, whereas LDs offer 30 to 70 percent electro-optical conversion efficiency. However, LEDs are much less expensive than LDs, which is why most commercial systems use them.

Two types of low-capacitance silicon photodiodes are used for receivers: *positive intrinsic negative* (PIN) and avalanche. The simpler and less expensive PIN photodiode is typically used in receivers that operate in environments with bright illumination, whereas the more complex and expensive avalanche photodiode is used in receivers that must operate in environments where background illumination is weak. The difference in the two types of photodiodes is their sensitivity.

The PIN photodiode produces an electrical current in proportion to the amount of light energy projected onto it. Although the avalanche photodiode requires more complex receiver circuitry, it operates in much the same way as the PIN diode, except that when light is projected onto it, a slight amplification of the light energy occurs. This makes it more appropriate for weakly illuminated environments. The avalanche photodiode also offers a faster response time than the PIN photodiode.

Operating Performance

Current applications of infrared technology yield performance that matches or exceeds the data rate of wire-based LANs: 10 Mbps for Ethernet and 16 Mbps for token ring. However, infrared technology has a much higher performance potential—transmission systems operating at 50 and 100 Mbps have already been demonstrated.

Because of its limited range and inability to penetrate walls, nondirected infrared offers some measure of protection against eavesdropping. Even signals that go out windows are useless to eavesdroppers because they do not travel far and may be distorted by impurities in the glass as well as by the glass placement angle.

Infrared offers high immunity from *electromagnetic interference* (EMI), which makes it suitable for operation in harsh environments like factory floors. Because of its limited range and inability to penetrate walls, several infrared LANs may operate in different areas of the same building without interfering with each other. Because there is less chance of multipath fading (large fluctuations in the received signal amplitude and phase), infrared links are highly robust.

Many indoor environments have incandescent or fluorescent lighting, which induces noise in infrared receivers. This is overcome by using directional infrared transceivers with special filters to reject background light.

Media Access Control (MAC)

Infrared supports both contention-based and deterministic MAC techniques, making it suitable for Ethernet as well as token ring LANs.

To implement Ethernet's contention protocol, *carrier sense multiple access* (CSMA), each computer's infrared transceiver is typically aimed at the ceiling. Light bounces off the reflector in all directions to enable each user to receive data from other users (see Figure 1-5). CSMA ensures that only one station can transmit data at a time. Only the station(s) to which packets are addressed can actually receive them.

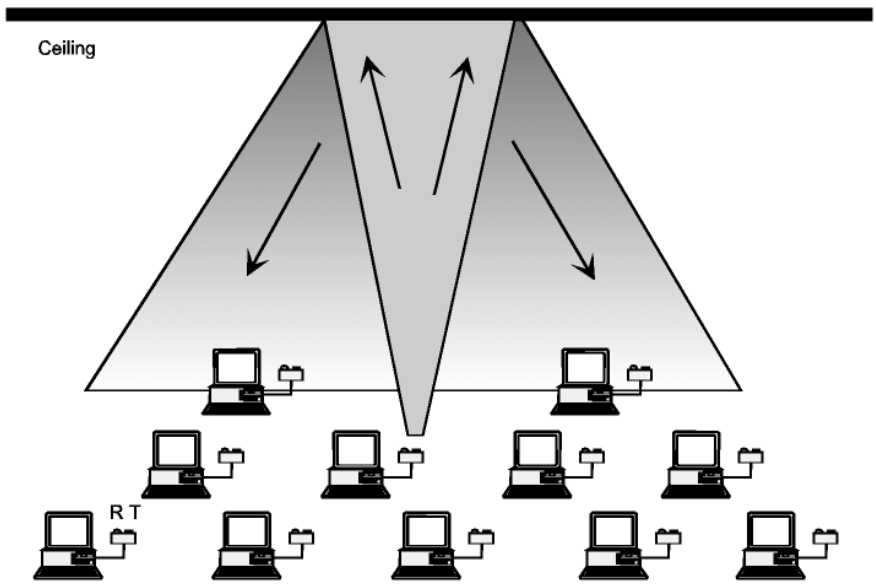

Figure 1-5
The implementation of Ethernet using diffuse infrared

Deterministic MAC relies on token passing to ensure that all stations in turn have an equal chance to transmit data. This technique is used in token ring LANs, where each station uses a pair of highly directive (line-of-sight) infrared transceivers. The outgoing transducer is pointed at the incoming transducer of a station down line, thus forming a closed ring with the wireless infrared links among the computers (see Figure 1-6). With this configuration, much higher data rates can be achieved because of the gain associated with the directive infrared signals. This approach improves the overall throughput, since fewer bit errors will occur, which minimizes the need for retransmissions.

Infrared Computer Connectivity

Most notebook computers and PDAs have infrared ports, and just about every major mobile phone brand includes at least one infrared-enabled handset. Infrared products for computer connectivity conform to the standards developed by the *Infrared Data Association* (IrDA). The standard

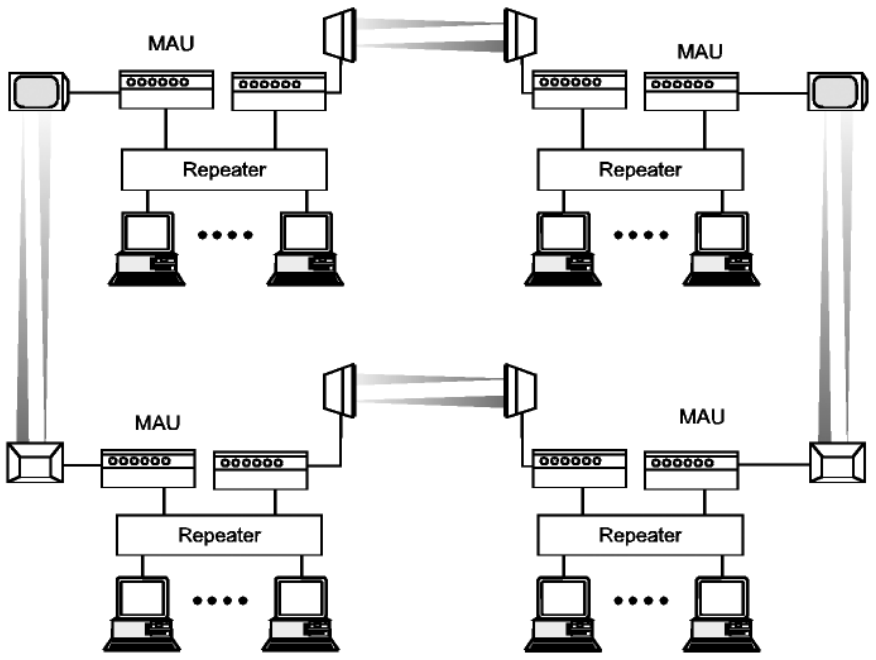

Figure 1-6
The implementation of token ring using line-of-sight infrared

protocols include *Serial Infrared* (SIR) at 115 Kbps, *Fast Infrared* (FIR) at 4 Mbps, and *Very Fast Infrared* (VFIR) at 16 Mbps. The higher speed available with VFIR is intended to address the new demands of transferring large image files between digital cameras, scanners, and PCs. Table 1-2 summarizes the performance characteristics of the IrDA's infrared standard.

Infrared's primary impact will take the form of benefits for mobile professional users. It enables simple point-and-shoot connectivity between devices to enable users to exchange information and reap more of the productivity gains promised by portable computing. IrDA technology is supported in over 100 million electronic devices including desktop, notebook, and palm PCs; printers; digital cameras; public phones/kiosks; cellular phones; pagers; PDAs; electronic books; electronic wallets; and other mobile devices.

When used on a LAN, infrared technology also confers substantial benefits to network administrators. Infrared is easy to install and configure, requires no maintenance, and imposes no remote-access tracking hassles. It does not disrupt other network operations, and it provides data security. Because it makes connectivity so easy, it encourages the use of high-productivity network and groupware applications, thus helping administrators amortize the costs of these packages across a larger user base.

Table 1-2

Performance characteristics of the IrDA's infrared standard

Feature/Function	Performance
Connection type	Infrared, narrow beam (30° angle or less).
Spectrum	Optical, 850 nm.
Transmission power	100 mW.
Data rate	Up to 16 Mbps using VFIR.
Range	Up to 3 feet (1 meter).
Supported devices	Two.
Data security	The short range and narrow angle of the infrared beam provide a simple form of security; otherwise, no security capabilities exist at the link level.
Addressing	Each device has a 32-bit physical ID that is used to establish a connection with another device.

Points of Convergence

In some ways, Bluetooth competes with infrared; in other ways, the two technologies are complementary. With both infrared and Bluetooth, data exchange is considered to be a fundamental function. Data exchange can be as simple as transferring business card information from a mobile phone to a palmtop, or as sophisticated as synchronizing personal information between a palmtop and desktop PC. In fact, both technologies can support many of the same applications, which raises the following question: Why would users need both technologies?

The answer lies in the fact that each technology has advantages and disadvantages. The very scenarios that leave infrared falling short are the ones where Bluetooth excels, and vice versa. Take the electronic exchange of business card information between two devices. This application will usually take place in a conference room or exhibit floor where a number of other devices might be attempting to do the same thing. Infrared excels in this situation. The short range and narrow angle of infrared—30° or less—enable each user to aim his or her device at the intended recipient with point-and-shoot ease. Close proximity to another person is natural in a business card exchange situation, as is pointing one device at another. The limited range and narrow angle of infrared enable other users to perform a similar activity with ample security and no interference.

In the same situation, a Bluetooth device would not perform as well as an infrared device. With its omnidirectional capability, the Bluetooth device must first discover the intended recipient. The user cannot simply point at the intended recipient—a Bluetooth device must perform a discovery operation that will probably reveal several other Bluetooth devices within range, so close proximity offers no advantage here. The user will be forced to select from a list of discovered devices and apply a security mechanism to prevent unauthorized access. All this makes the use of Bluetooth for business card exchange an awkward and needlessly time-consuming process.

In other data exchange situations, however, Bluetooth might be the preferred choice. Bluetooth's capability to penetrate solid objects and communicate with other devices in a piconet allows for data exchange opportunities that are very difficult or impossible with infrared. For example, Bluetooth enables a user to synchronize a mobile phone with a notebook computer without taking the phone out of the user's jacket pocket or purse. This enables the user to type a new address at the computer and move it to the mobile phone's directory without unpacking the phone and setting up a

cable connection between the two devices. The omnidirectional capability of Bluetooth enables synchronization to occur instantly, assuming that the phone and computer are within 30 feet of each other.

Using Bluetooth for synchronization does not require that the phone remain in a fixed location. If a phone is carried about in a briefcase, the synchronization can occur while the user moves around. This is not possible with infrared because the signal is not able to penetrate solid objects and the devices must be within a few feet of each other. Furthermore, the use of infrared requires that both devices remain stationary while the synchronization occurs.

When it comes to data transfers, infrared does offer a significant speed advantage over Bluetooth. Whereas Bluetooth moves data between devices at an aggregate rate of 1 Mbps, infrared offers up to 16 Mbps. Even when Bluetooth is enhanced for higher data rates in the future, infrared is likely to maintain its speed advantage for many years to come.

Bluetooth complements infrared's point-and-shoot ease of use with omnidirectional signaling, longer-distance communications, and the capacity to penetrate walls. For some users, having both Bluetooth and infrared will provide the optimal short-range wireless solution. For others, the choice of adding Bluetooth or infrared will be based on the applications and intended usage.

Home Radio Frequency (HomeRF)

Telecommuters are becoming increasingly interested in connecting computers and peripherals at home, possibly tying in their notebooks from work as well, so they can access the Internet or corporate intranet from a shared broadband connection like *Digital Subscriber Line* (DSL) or cable. One method of implementing a wireless network in the home is to use products that adhere to the standards of the *Home Radio Frequency Working Group* (HomeRF WG).

HomeRF is positioned as a global extension of *Digitally Enhanced Cordless Telephony* (DECT), the popular cordless phone standard that enables different brands to work together so certified handsets from one vendor can communicate with base stations from another. DECT has been largely confined to Europe because its native 1.9 GHz frequency band requires a license elsewhere, but HomeRF extends DECT to other regions by using the license-free 2.4 GHz frequency band, which is also used by Bluetooth and

WiFi. HomeRF also adds functionality by blending several industry standards, including IEEE 802.11 FHSS for data and DECT for voice.

The standards for HomeRF are addressed by a consortium of vendors called the HomeRF WG. Under the HomeRF standard, compliant devices carry both voice and data traffic and interoperate with the *Public Switched Telephone Network* (PSTN) and the Internet. The standard specifies the use of *Time Division Multiple Access* (TDMA) to provide the delivery of interactive voice and other time-critical services, as well as *carrier sense multiple access/collision avoidance* (CSMA/CA) for the delivery of high-speed packet data. Table 1-3 summarizes the main characteristics of HomeRF.

Applications

The HomeRF standard provides the basis for a broad range of home networking applications, including the following:

- Shared access to the Internet from anywhere in the home, enabling a user to browse the Web from a notebook on the deck or have stock quotes delivered to a PC in the den

Table 1-3

HomeRF characteristics

Feature/Function	Performance
Frequency-hopping network	50 hops per second
Frequency range	2.4 GHz ISM band
Transmission power	100 mW
Data rate	1.6 Mbps with HomeRF 1.0 10 Mbps with HomeRF 2.0 25 Mbps with HomeRF 3.0 (future)
Range	Covers up to 150 feet for typical home and yard
Total network devices	Up to 127
Voice connections	Up to 4 active handsets
Data security	Blowfish encryption algorithm (over 1 trillion codes)
Data compression	LZRW3-A algorithm
48-bit network ID	Enables concurrent operation of multiple co-located networks

- Automatic intelligent routing of incoming telephone calls to one or more cordless handsets, fax machines, or voice mailboxes of individual family members
- Cordless handset access to an integrated message system to review stored voice mail, faxes, and e-mail
- WLANs, enabling users to share files and peripherals between one or more PCs, no matter where they are located within the home
- Spontaneous control of security, electrical, heating, and air conditioning systems from anywhere in or around the home
- Multiuser computer games playable in the same room or in multiple rooms throughout the home

Network Topology

The HomeRF system can operate either as an ad hoc network or as a managed network under the control of a *connection point*. In an ad hoc network, where only data communication is supported, all stations are equal and control of the network is distributed between the stations. For time-critical communications such as interactive voice, a *connection point* is required to coordinate the system. The connection point, which provides the gateway to the PSTN, can be connected to a PC via a standard interface that will enable enhanced voice and data services such as the *universal serial bus* (USB). The HomeRF system also can use the connection point to support power management for prolonged battery life by scheduling device wakeup and polling. The network can accommodate a maximum of 127 nodes. The nodes consist of four basic types:

- A connection point that supports voice and data services
- A voice terminal that only uses the TDMA service to communicate with a base station
- A data node that uses the CSMA/CA service to communicate with a base station and other data nodes
- An integrated node that can use both TDMA and CSMA/CA services

HomeRF uses intelligent hopping algorithms that detect wideband, static interference from microwave ovens, cordless phones, baby monitors, and WiFi networks. Once detected, the HomeRF hop algorithm adapts so no two consecutive hops occur within this interference range. This means that, with very high probability, a packet lost due to interference will get through

when it retries on the next hop. Although these algorithms benefit data applications, they are especially important for voice, which requires extremely low *bit error rates* (BER) and low latency. WiFi does not use the frequency-hopping mechanism; instead, it uses DSSS. In doing so, however, WiFi does not support real-time applications such as voice, and it is not very resistant to interference from other household devices. Standards currently under development for WiFi are addressing these issues.

Future Plans

Work has already begun on the future HomeRF 2.1 specification, which will add features designed to reinforce its advantages for voice. Planned enhancements also will enable HomeRF to run WiFi, leading to a peaceful coexistence between the two and giving users the added functionality of HomeRF.

HomeRF 2.0 already supports up to eight phone lines, eight registered handsets, and four active handsets with voice quality and range comparable to leading 2.4 GHz phone systems. With that many lines, each family member can have a personal phone number. HomeRF 2.1 plans to increase the number of active handsets with the same or better voice quality, thus supporting the needs of small businesses.

The 150-foot range of HomeRF already covers most homes into the yard. HomeRF 2.1 will extend that range for larger homes and businesses by using wireless repeaters that are similar to enterprise access points but without the need to connect each one to Ethernet. HomeRF frequency-hopping technology also avoids the complexity of assigning *radio frequency* (RF) channels to multiple APs (or repeaters), and offers easy and effective security and interference immunity. This is especially important because households and small businesses do not usually have network administrators.

To enable individuals to roam across very large homes and fairly large offices while talking on the phone and without losing their voice connection, HomeRF 2.1 will also support voice roaming with soft handoff between repeaters.

HomeRF 2.0 supports Ethernet speeds up to 10 Mbps with fallback speeds and backward compatibility to earlier versions of HomeRF. Performance can be further enhanced to about 20 Mbps. The HomeRF WG is evaluating the need for such enhancements at 2.4 GHz in light of its planned support of WiFi at 5 GHz.

A proposed change to the *Federal Communications Commission's* (FCC's) Part 15 rules governing the 2.4 GHz ISM band will allow adaptive frequency hopping. Although these proposed techniques are not legal today,

they enable hoppers such as Bluetooth and HomeRF to recognize and avoid interference from static frequency technologies such as WiFi. Because HomeRF already adjusts its hopping pattern based on interference to ensure that two consecutive hops do not land on interference, supporting this FCC proposal seems trivial.

The HomeRF WG believes in the peaceful coexistence of 2.4 and 5 GHz since each frequency band and technology has specific strengths that complement each other. Rather than draft a specification for 5 GHz, the group simply endorses 802.11a (also known as *WiFi5*) for high-bandwidth applications such as high-definition video streaming and MPEG2 compression. It plans to write application briefs describing how to bridge between 2.4 and 5 GHz technologies, including how to handle differences in *quality of service* (QoS).

Home users have a need for a wireless network that is easy to use, cost effective, and spontaneously accessible. It should also be able to carry voice and data communications. Certified HomeRF products are available today from consumer brands such as Compaq, Intel, Motorola, Proxim, and Siemens through retail, online, and service provider channels. They come in a variety of form factors such as USB and PC Card adapters, residential gateways, and a growing variety of devices that embed HomeRF.

Windows XP does not include integral support for HomeRF. Instead, Microsoft chose to have XP integrally support WiFi, which many industry analysts believe will eventually overtake HomeRF. Even Intel, an early supporter of HomeRF, is now focused exclusively on WiFi. Furthermore, with the growing popularity of Wi-Fi, it is unlikely that users will want to have two technologies—one for the office and another for home. With no appreciable price difference between the two, telecommuters are more likely to standardize on the technology they use in the workplace.

WiFi

As noted earlier, WiFi refers to a version of Ethernet specified under the IEEE 802.11a and 802.11b standards for LANs operating in the 5 GHz and 2.4 GHz unlicensed frequency bands, respectively. WiFi is equally suited to businesses of all types and sizes as well as their telecommuting and remote employees working at home or in branch offices. Equipment is available that enables both bands to be used to support separate networks simultaneously. Some APs, for example, come with dual slots for 2.4 and 5 GHz radio cards, supporting devices on both networks at the same time.

The 802.11 standard makes the wireless network a straightforward extension of the wired network. This has allowed for a very simple implementation of wireless communication with obvious benefits—these can be installed using the existing network infrastructure with minimal retraining or system changes. Notebook users can work anywhere in a building or campus while remaining in contact with the network via strategically placed APs that are plugged into the wired network. Likewise, PDA users can roam throughout the workplace and stay in contact with the corporate network via the same APs, giving them high-speed access to the Internet, e-mail, and network resources. Users can also hot sync their data as they move about, so their information is always up-to-date.

Wireless users can run the same network applications they use on an Ethernet LAN. For most users, no noticeable functional difference exists between a wired Ethernet desktop computer and a wireless computer equipped with a wireless adapter other than the added benefit of the ability to roam within the wireless cell. Under many circumstances, it may be desirable for mobile network devices to link to a conventional Ethernet LAN in order to use servers, printers, or an Internet connection supplied through the wired LAN. A wireless AP is one device that can be used to provide this link.

The IEEE 802.11b standard designates devices that operate in the 2.4 GHz band to provide a data rate of up to 11 Mbps at a range of up to 300 feet (100 meters) indoors and 1,800 feet (600 meters) outdoors using DSSS technology. But with high-gain, line-of-sight antennas, a range of up to 50 miles is possible. Some vendors have implemented proprietary extensions to the 802.11b standard, allowing applications to burst beyond 11 Mbps to reach as much as 22 Mbps. Users can share files and applications, exchange e-mail, access printers, share access to the Internet, and perform any other task as if they were directly cabled to the network.

The IEEE 802.11a standard designates devices that operate in the 5 GHz band to provide a data rate of up to 54 Mbps at a range of up to 900 feet (300 meters) indoors using DSSS technology. Sometimes called WiFi5, this amount of bandwidth enables users to transfer large files quickly or even watch a movie in MPEG format over the network without noticeable delays. This technology works by transmitting high-speed digital data over a radio wave utilizing *orthogonal frequency division multiplexing* (OFDM) technology.

OFDM works by splitting the radio signal into multiple smaller subsignals, which are then transmitted simultaneously at different frequencies to the receiver. OFDM reduces the amount of interference in signal transmissions, which results in a high-quality connection. WiFi5 products automat-

ically sense the best possible connection speed to ensure the greatest speed and range possible with the technology. Some vendors have implemented proprietary extensions to the 802.11a standard, enabling applications to burst beyond 54 Mbps to reach as much as 72 Mbps.

WiFi networks can be implemented in infrastructure mode or ad hoc mode. In infrastructure mode—referred to in the IEEE specification as the *basic service set*—each wireless client computer associates with an AP via a radio link. The AP connects to the 10/100 Mbps Ethernet enterprise network using a standard Ethernet cable and provides the wireless client computer with access to the wired Ethernet network. Ad hoc mode is the peer-to-peer network mode, which is suitable for very small installations. Ad hoc mode is referred to in the 802.11b specification as the *independent basic service set*.

Security for WiFi networks is handled by the IEEE standard called *Wired Equivalent Privacy* (WEP), which is commonly available in 64- and 128-bit versions. The more bits in the encryption key, the more difficult it is for hackers to decode the data. It was originally believed that 128-bit encryption would be virtually impossible to break due to the large number of possible encryption keys. However, hackers have since developed methods to break 128-bit WEP without having to try each key combination, proving that this system is not totally secure. These methods are based upon the ability to gather enough packets off the network using special eavesdropping equipment to determine the encryption key. Although WEP can be broken, it does take considerable effort and expertise to do so. To help thwart hackers, WEP should be enabled on all wireless devices and the keys should be rotated on a frequent basis.

The WLAN industry has recognized that WEP is not as secure as it was once thought and is responding by developing another standard, known as 802.11i, which will enable WEP to use the *Advanced Encryption Algorithm* (AES) to make the encryption key even more difficult to determine. AES replaces the older 56-bit *Digital Encryption Standard* (DES), which had been in use since the 1970s. AES can be implemented in 128-, 192-, and 256-bit versions. For a computer with enough processing power to test 255 keys per second, it would take 149 trillion years to crack AES.

WiFi is a certification of interoperability awarded by the WiFi Alliance, formerly known as the *Wireless Ethernet Compatibility Alliance* (WECA). The WiFi seal indicates that a device has passed independent tests and will reliably interoperate with all other WiFi-certified equipment. Customers benefit from this standard by avoiding becoming locked into one vendor's solution—they can purchase WiFi-certified AP and client devices from different vendors and still expect them to work together.

Table 1-4
WiFi characteristics

Feature/Function	Performance
Frequency range	2.4 and 5 GHz ISM band.
Transmission power	100 mW.
Data rate	11 Mbps at 2.4 GHz and 54 Mbps at 5 GHz. 54 Mbps at 2.4 GHz under 802.11g (future).
Range	2.4 GHz systems: indoors at up to 300 feet (100 meters) from the client to AP; outdoors at up to 1,800 feet (600 meters) between antennas. 5 GHz systems: indoors at up to 900 feet (275 meters) from the client to AP; outdoors at up to 5,400 feet (1,800 meters) between antennas.
Total network devices	Up to 255 client devices may be associated with an AP, with 128 in simultaneous operation.
Voice connections	*Voice over Internet Protocol* (VoIP) (future)
Data security	Authentication: shared key or open key. Encryption: WEP at 64 bits or 128 bits for 2.4 GHz systems plus 152 bits for 5 GHz systems.
Modulation	2.4 GHz systems: DSSS. 5 GHz systems: OFDM.
48-bit network ID	Enables the concurrent operation of multiple co-located networks.

General Packet Radio Service (GPRS)

Analog cellular mobile phone systems are considered *first-generation* (1G) technology, whereas digital cellular mobile phone systems are referred to as *second-generation* (2G) technology. The next generation of cellular services offers a broadband data capability and is known simply as *3G*, for *third-generation* technology. When fully implemented, 3G technologies will make it possible for service providers to offer a variety of mobile services ranging from messaging to speech, data and video communications, Internet and intranet access, and high bit rate communication up to 2 Mbps.

Many carriers have already taken an interim step to 3G, referred to as *2.5G*, which uses IP to provide fast access to data networks via GPRS tech-

nology. Compared to *Circuit-Switched Data* (CSD), which operates at up to 14.4 Kbps, and *High-Speed Circuit-Switched Data* (HSCSD), which operates at up to 43.2 Kbps, GPRS utilizes packet-switching technology to transmit short bursts of data over an IP-based network to deliver speeds of up to 144 Kbps over an always-on wireless connection.

True 3G networks based on *Enhanced Data Rates for GSM Evolution* (EDGE) technology deliver data at speeds of up to 384 Kbps. Carriers in the United States have been moving toward 3G for several years by overlaying various technologies onto their existing networks to enhance their data-handling capabilities.

For carriers with TDMA-based networks, the first step to offering true 3G services is to deploy *Global Systems for Mobile communications* (GSM) and then GPRS. The new GSM/GPRS networks do not replace existing TDMA networks; carriers will continue supporting these networks long into the future to service their voice customers. Eventually, all TDMA customers will be migrated to GSM/GPRS. Once the GSM/GPRS overlay is in place in a market, the carriers can upgrade their networks with EDGE-compliant software to boost data transmission rates to as much as 384 Kbps and begin the availability of true 3G services.

Carriers whose wireless networks are based on *Code Division Multiple Access* (CDMA) will take a different technology path to 3G, going through CDMA2000, before eventually arriving at *Wideband CDMA* (W-CDMA). Both EDGE and W-CDMA offer a migration path to the global standard *Universal Mobile Telecommunications System* (UMTS).

Coverage for 2.5/3G services is still ramping up, despite the impressive figures thrown out by individual carriers. The next step is for service providers to engage in more roaming arrangements, which is a way to save costs, reduce time to market, and add value to attract more customers.

The data speed of 2.5/3G services is determined by many factors, including the equipment and software in the wireless network, the distance of the user from the nearest base station, and how fast the user may be moving. The claimed speed of the service is rarely, if ever, achieved in the real-world operating environment.

The pricing plans and price points differ by carrier, from a simple add-on to the existing digital voice plans for a basic data service to tiered pricing plans based on actual data usage. Depending on the applications, users can opt for 2.5/3G cell phones with multimedia messaging capabilities. Alternatively, users with heavy messaging and file transfer requirements may opt for PC Cards for notebooks and PDAs.

Some service providers intend to support WiFi as well as GPRS, viewing them as complementary. The existing GPRS and upcoming EDGE networks provide wide area coverage for applications where customers want brief access to applications such as their e-mail and calendar, whereas WiFi networks will be available in convenient locations where customers are likely to spend time accessing larger data files and browsing the Web. Service providers will offer seamless access to 3G and WiFi networks via one PC Card (see Figure 1-7) and bill customers for both services with one invoice.

Like WiFi, one of the characteristics of 3G wireless technology is always-on high-speed mobile Internet connection. Lucent Technologies has demonstrated the successful seamless hand-off of a wireless data call from a WiFi to a GSM-based 3G network and WiFi to a CDMA2000-based 3G network, enabling mobile laptop users to browse the Internet while roaming between the two network types with no interruption in the session. The capabilities rely on the Mobile IP standard from the *Internet Engineering Task Force* (IETF). Mobile IP supports intertechnology handoffs between WiFi and 3G technologies. As a future service, this will enhance mobile workers' wireless experience by giving them continuous access to the information they need using the fastest technology available in any given location, greatly extending the wireless coverage area.

Figure 1-7
Nokia offers the D211 GSM card, providing GPRS and WLAN connectivity in one. Another version of the product, the D311, is designed for the North American market. Drivers are available for PocketPC, Windows, and Linux.

Fixed Wireless Access

Fixed wireless access technology provides a wireless link to the PSTN using spectrum licensed by the FCC. It constitutes an alternative to traditional wire-based local telephone service. Since calls and other information (for example, data and images) are transmitted through the air rather than through conventional cables and wires, the cost of providing and maintaining telephone poles and cables is avoided. Unlike cellular technologies, which provide services to mobile users, fixed wireless services require a rooftop antenna to an office building or home, which is lined up with a service provider's hub antenna. Although WiFi is set up in a similar manner, it uses unlicensed spectrum and does not provide connectivity with telephone networks.

Fixed wireless access systems come in two varieties: narrowband and broadband. A narrowband fixed wireless access service can provide bandwidth up to 128 Kbps, which can support one voice conversation and a data session such as Internet access or fax transmission. A broadband fixed wireless access service can provide bandwidth in the multimegabit-per-second range, which is enough to support telephone calls, television programming, and broadband Internet access.

A narrowband fixed wireless service requires a wireless access unit, which is installed on the exterior of a home or business (see Figure 1-8) to enable customers to originate and receive calls without changing their

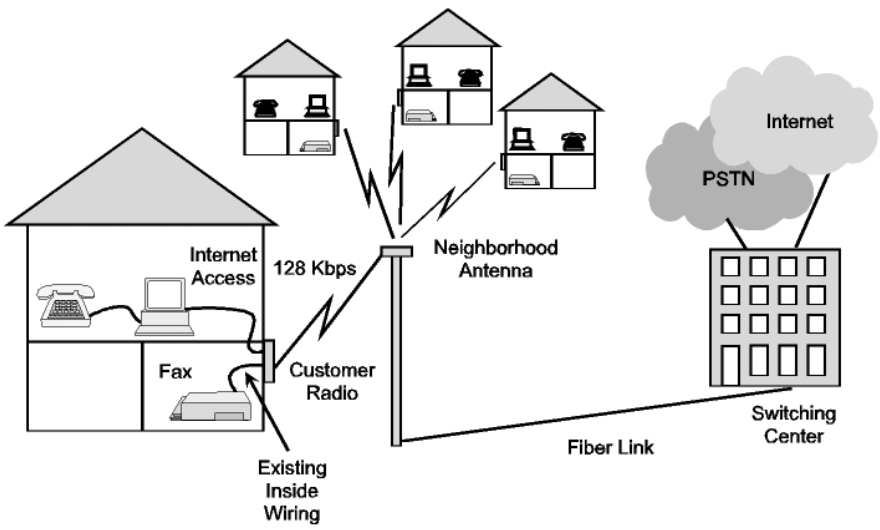

Figure 1-8
A simple fixed wireless configuration for a narrowband access service

existing analog telephones. This transceiver is positioned to provide an unobstructed view to the nearest base station receiver. Voice and data calls are transmitted from the transceiver at the customer's location to the base station equipment, which relays the call through carrier's existing network facilities to the appropriate destination. No investment in special phones or facsimile machines is required; customers use all their existing equipment.

Narrowband fixed wireless systems use the licensed 3.5 GHz radio band with 100 MHz spacing between the uplink and downlink frequencies. Subscribers receive network access over a radio link within a range of 200 meters (600 feet) to 40 kilometers (25 miles) of the carrier's hub antenna. About 2,000 subscribers can be supported per cell site.

Broadband fixed wireless access systems are based on microwave technology. *Multichannel Multipoint Distribution Service* (MMDS) operates in the licensed 2 to 3 GHz frequency range, whereas *Local Multipoint Distribution Service* (LMDS) operates in the licensed 27 to 31 GHz frequency range. Both services are used by *Competitive Local Exchange Carriers* (CLECs) primarily to offer broadband Internet access, but they are also capable of supporting voice. These technologies are used to bring voice and data traffic to the fiber-optic networks of *Interexchange Carriers* (IXCs) and nationwide CLECs, bypassing the local loops of the *Incumbent Local Exchange Carriers* (ILECs).

Even if a business subscribes to MMDS or LMDS, it can still use WiFi within a building or campus environment. Once the traffic moves from the WiFi link to the wired LAN via an AP, it can go out to an MMDS/LMDS link via a hub or switch. The customer's hub or switch would be connected to a *network interface unit* (NIU), which is cabled to a rooftop MMDS/LMDS antenna. That antenna sends the traffic to the service provider's hub antenna, which is cabled to an *Asynchronous Transfer Mode* (ATM) switch. That switch provides high-speed access to the Internet (see Figure 1-9).

LMDS

This broadband service enables communications providers to offer a variety of high-bandwidth services to homes and businesses, including broadband Internet access. LMDS offers greater bandwidth capabilities than MMDS, but has a maximum range of only 7.5 miles from the carrier's hub to the customer premises. This range can be extended, however, through the use of optical fiber links.

LMDS provides enormous bandwidth: enough to support 16,000 voice conversations plus 200 channels of television programming. CLECs can

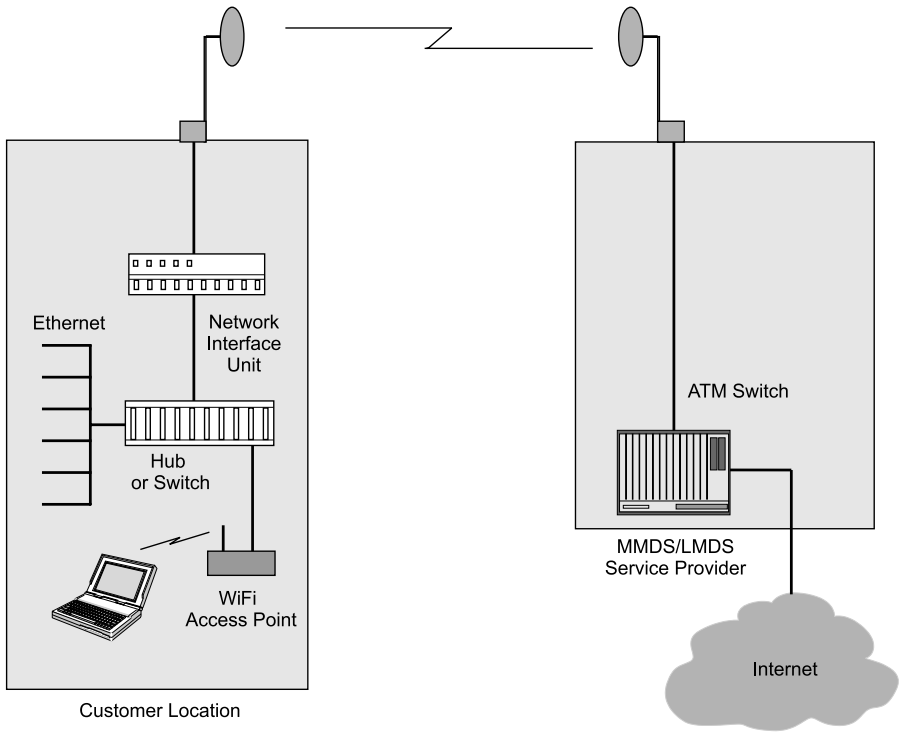

Figure 1-9
Data from a WiFi connection can reach the Internet through other wireless connections, such as MMDS or LMDS.

deploy LMDS to completely bypass the local loop, eliminating access charges and avoiding service-provisioning delays. Because the service entails setting up equipment between the provider's hub location and customer buildings for the microwave link, LMDS costs far less to deploy than installing new fiber. This enables CLECs to economically bring customer traffic onto their existing metropolitan fiber networks and, from there, to a national backbone network.

The strategy among many CLECs is to offer LMDS to owners of multitenant office buildings and then install cable to each tenant who subscribes to the service. The cabling goes to an on-premises switch, which is run to the antenna on the building's roof. That antenna is aimed at the service provider's antenna at its hub location. The line-of-sight wireless link between the two antennas offers a broadband pipe for multiple voice, data, and video applications. Subscribers can use LMDS for a variety of high-bandwidth applications, including television broadcast, videoconferencing, LAN interconnection, broadband Internet access, and telemedicine.

LMDS operation requires a clear line of sight between the carrier's hub station antenna and the antenna at each customer location. However, LMDS is also capable of operating without having a direct line of sight with the receiver. This feature, which is highly desirable in built-up urban areas, may be achieved by bouncing signals off buildings so that they get around obstructions. At the receiving location, the data packets arriving at different times are held in queue for resequencing before they are passed to the application. This scheme does not work well for voice, however, because the delay resulting from queuing and resequencing disrupts two-way conversation.

A roof-mounted multisectored antenna is placed at the carrier's hub location. Each sector of the antenna receives/transmits signals between itself and a specific customer location. This antenna is very small, often measuring only 12 inches in diameter. The hub antenna brings the multiplexed traffic down to an indoor switch, which processes the data into 53-byte ATM cells for transmission over the carrier's fiber network. These individually addressed cells are converted back to their native format before going off the carrier's network to their proper destinations—the Internet, PSTN, or the customer's remote location.

Each customer's location has a rooftop antenna that sends/receives multiplexed traffic. This traffic passes through an indoor NIU, which provides the gateway between the RF components and the in-building equipment, such as a LAN hub, *private branch exchange* (PBX), or videoconferencing system. The NIU includes an up/down converter that changes the frequency of the microwave signals to a lower *intermediate frequency* (IF) that the electronics in the office equipment can more easily (and inexpensively) manipulate.

A potential problem for LMDS users is that the signals can be disrupted by heavy rainfall and dense fog—even foliage can block a signal. In metropolitan areas where new construction is a fact of life, a line-of-sight transmission path can disappear virtually overnight. For these reasons, many IT executives are leery of trusting mission-critical applications to this wireless technology. Service providers downplay this situation by claiming that LMDS is just one local access option and that fiber links are the way to go for mission-critical applications. In fact, some LMDS providers offer fiber as a backup in case the microwave links experience interference.

There is controversy in the industry about the economics of the point-to-multipoint architecture of LMDS. Some experts claim that the business model of going after low-usage customers is fundamentally flawed and will never justify the service provider's cost of equipment, installation, and provisioning. With an overabundance of fiber in the ground and metropolitan area Gigabit Ethernet services coming online at a competitive price, the

time for LMDS may have come and gone. In addition, newer wireless technologies like free-air laser hold a significant speed advantage over LMDS, as do submillimeter transmission in the 60 and 95 GHz bands.

Fiber optics is the primary transmission medium for broadband connectivity today. However, of the estimated 4.6 million commercial buildings in the United States, 99 percent are not served by fiber. Businesses are at a competitive disadvantage in today's information-intensive world unless they have access to broadband access services, including high-speed Internet access. These businesses, including many data-intensive high-technology companies, can be adequately served with LMDS. Despite the financial problems of LMDS providers, the technology has the potential to become a significant portion of the global access market, which will include a mix of many technologies, including DSL, cable modems, broadband satellite, and fiber-optic systems.

MMDS

This microwave technology traces its origins to 1972 when it was introduced to provide an analog service called *Multipoint Distribution Service* (MDS). For many years, MMDS was used for the one-way broadcast of television programming, but in early 1999, the FCC opened up this spectrum to allow two-way transmissions, making it useful for delivering telecommunication services, including high-speed Internet access to homes and businesses.

This technology, which has now been updated to digital, operates in the 2 to 3 GHz range, enabling large amounts of data to be carried over the air from the operator's antenna towers to small receiving dishes installed at each customer location. The useful signal range of MMDS is about 30 miles, which beats LMDS at 7.5 miles and DSL at 18,000 feet. Furthermore, MMDS is easier and less costly to install than cable service.

With MMDS, a complete package of television programs can be transmitted to homes and businesses. Because MMDS operates within the frequency range of 2 to 3 GHz, which is much lower than LMDS at 28 to 31 GHz, it can support only up to 24 stations. However, operating at a lower frequency range means that the signals are not as susceptible to interference as those using LMDS technology.

Most of the time the operator receives television programming via a satellite downlink. Large satellite antennas installed at the head end collect these signals and feed them into encoders that compress and encrypt the programming. The encoded video and audio signals are modulated via *amplitude modulation* (AM) and *frequency modulation* (FM), respectively,

to an IF signal. These IF signals are up-converted to MMDS frequencies, and then amplified and combined for delivery to a coax cable, which is connected to the transmitting antenna. The antenna can have an omnidirectional or sectional pattern.

The small antennas at each subscriber location receive the signals and pass them via a cable to a set-top box connected to the television. If the service also supports high-speed Internet access, a cable also goes to a special modem connected to the subscriber's PC. MMDS sends data as fast as 10 Mbps downstream (toward the computer). Typically, service providers offer downstream rates of 512 Kbps to 2.0 Mbps, with burst rates up to 5 Mbps whenever spare bandwidth becomes available.

Originally, there was a line-of-sight limitation with MMDS technology. But this has been overcome with a complementary technology called *vector orthogonal frequency division multiplexing* (VOFDM). Because MMDS does not require an unobstructed line of sight between antennas, signals bouncing off objects en route to their destination require a mechanism for being reassembled in their proper order at the receiving site. VOFDM handles this function by leveraging multipath signals, which normally degrade transmissions. It does this by combining multiple signals at the receiving end to enhance or recreate the transmitted signals. This increases the overall wireless system performance, link quality, and availability. It also increases service providers' market coverage through non-line-of-sight transmission.

MMDS equipment can be categorized into two types based on the duplexing technology used: *frequency division duplexing* (FDD) or TDD. Systems based FDD are good solutions for voice and bidirectional data because forward and reverse use separate and equally large frequency bands. However, the fixed nature of this scheme limits the overall efficiency when used for Internet access. This is because Internet traffic tends to be bursty and asymmetrical. Instead of preassigning bandwidth with FDD, Internet traffic is best supported by a more flexible bandwidth allocation scheme.

This is where TDD comes in; it is more efficient because each radio channel is divided into multiple time slots through TDMA technology, which enables multiple channels to be supported. Because TDD has flexible time slot allocations, it is better suited for data delivery—specifically, Internet traffic. TDD enables service providers to vary uplink and downlink ratios as they add customers and services. Many more users can be supported by the allocation of bandwidth on a nonpredefined basis.

MMDS is being used to fill the gaps in market segments where cable modems and DSL cannot be deployed because of distance limitations and

cost concerns. Like these technologies, MMDS provides data services and enhanced video services such as video on demand as well as Internet access. MMDS can be another access method to complement a carrier's existing cable and DSL infrastructure, or it can be used alone for direct competition. With VOFDM technology, MMDS is becoming a workable option that can be deployed cost effectively to reach urban businesses that do have line-of-sight access, and in suburban and rural markets for small businesses and telecommuters.

Fixed wireless access technology originated out of the need to contain carriers' operating costs in rural areas, where pole and cable installation and maintenance are more expensive than in urban and suburban areas. However, wireless access technology can also be used in urban areas to bypass the LEC for long-distance calls. Since the IXC or CLEC avoids having to pay the ILEC's local loop interconnection charges, the savings can be passed back to the customer. This arrangement is also referred to as a *wireless local loop* (WLL).

Laser Transmission

A relatively new category of wireless communication uses laser, sometimes called *free-space optics*, operating in the near-infrared region of the light spectrum. Utilizing coherent laser light, these wireless line-of-sight links are used to link buildings in campus environments and urban areas where the installation of cable is impractical and the performance of leased lines is too slow.

Laser links between sites can be operated at the full LAN channel speed. In addition, unlike microwave transmission, laser transmission does not require an FCC license, and data traveling by laser beam cannot be intercepted. Via an AP to the wired LAN, WiFi traffic within a building can go out a hub or switch connected to the laser system. From there, the data is beamed to another building's laser system connected to its LAN.

The lasers at each location are aligned with a simple bar graph and tone lock procedure. Fiber-optic repeaters are used to connect the LANs to the laser units. Alternatively, a bridge equipped with a fiber-optic-to-AUI transceiver can be used (see Figure 1-10). Connections to and from the laser are made using standard fiber-optic cable, protecting data from sources of RF and EMI. Monitors can be attached to the laser units to provide operational status, such as signal strength, and to implement local and remote loopback diagnostics.

Figure 1-10
Terabeam Magna, a free-space optics system from TeraBeam Corporation

The reason why laser products are not used very often for business applications is because transmission is diminished by atmospheric conditions that produce effects such as absorption, scattering, and shimmer. All three can reduce the amount of light energy that is picked up by the receiver and corrupt the data being sent.

Absorption refers to the capability of various frequencies to pass through the air. Absorption is determined largely by the water vapor and carbon dioxide content of the air along the transmission path, which, in turn, depends on humidity and altitude. The gases that form in the atmosphere have many resonant bands, which enable specific frequencies of light to pass. These transmission windows occur at various wavelengths, such as the visible light range. Another window occurs at the near-infrared wavelength of approximately 820 nm. Laser products tuned to this window are not greatly affected by absorption.

Scattering has a much greater effect on laser transmission than absorption. The atmospheric scattering of light is a function of its wavelength and the number and size of scattering particles in the air. The optical visibility

along the transmission path is directly related to the number and size of these particles. Fog and smog are the main conditions that tend to limit visibility for optical-infrared transmission followed by snow and rain.

Shimmer is caused by localized differences in the air's index of refraction. This is caused by a combination of factors, including the time of day (daytime heat), terrain, cloud cover, wind, and the height of the optical path above the source of shimmer. These conditions cause fluctuations in the received signal level by directing some of the light out of its intended path. Beam fluctuations may degrade system performance by producing short-term signal amplitudes, which approach threshold values. Signal fades below these threshold values result in error bursts.

Vendors have taken steps to mitigate the effects of absorption, scattering, and shimmer. For example, techniques such as FM in the transmitter and an *automatic gain control* (AGC) in the receiver can minimize the effects of shimmer. Also, selecting an optical path several meters above heat sources can greatly reduce the effects of shimmer. However, all of these distorting conditions can vary greatly within a short time span or persist for long periods, requiring on-site expertise to constantly fine-tune the system.

Many businesses simply cannot risk frequent or extended periods of downtime while the necessary compensating adjustments are being made. As if all this was not enough, one must contend with other potential problems, such as thermal window coatings and the laser beam's angle of incidence, both of which can disrupt transmission. These problems are being overcome with newer lasers that operate in the 1,550 nm wavelength. A 1,550 nm delivery system is powerful enough to go through windows, can deliver signals under the fog blanket, and is safe enough that it does not blind the casual viewer who happens to look into the beam. Up to 1 Gbps of bandwidth is available with these systems—the equivalent bandwidth capacity of 660 T1 lines.

Laser also carries a distance limitation associated with laser. The link generally cannot exceed 1.5 km, and 1 km is preferred. With 1,550 nm systems, the practical distance of the link is only 500 meters. Despite its limitations, laser (or free-space optics) can provide a valuable last link between the fiber network and the end user—including serving as a backup to more conventional methods such as fiber. Free-space optics, unlike other transmission technologies, is not tied to standards or standards development. Vendors simply attach their equipment into existing fiber-based networks and then use any laser transmission methods they like. This encourages innovation, differentiation, and speed of deployment.

Conclusion

The emergence and proliferation of WiFi networks has become a phenomenal pull on broadband demand. In fact, the sudden success of WiFi has the FCC concerned that the airwaves may be getting too crowded, especially as *wireless Internet service providers* (WISPs) extend the range of WiFi to broaden their coverage areas. Amateur radio enthusiasts and some television stations, for example, claim that WiFi products are raising the level of interference on their transmissions. According to some interpretations of FCC regulations, since amateur radio and television stations are licensed, users of offending unlicensed WiFi gear must either eliminate the interference or shut down. Court cases have upheld this interpretation, which basically holds that licensed operators have preference over unlicensed operators.

As more devices come online to take advantage of WiFi, the FCC will come under more pressure to adopt measures that enable devices to peacefully coexist in the shared spectrum, such as reducing the power of 2.4 GHz devices to limit RF emissions or refining the definition of spread spectrum to make it less interfering. In the past, the FCC has even migrated operators from one spectrum band to another if it was deemed to be in the public interest. Judging by the impact it is already having on Internet users, it is more likely that the FCC will give preference to WiFi as it looks for ways to accommodate all users.