channels if they occupy frequencies outside their allocated frequency bands, although interference can be reduced by having a guard band between channels. Interference can also result from other users and other systems operating in the same frequency band. Certain filters and spread-spectrum techniques are used to eliminate this type of interference.

### 4.3.3 Capacity Limits of Wireless Channels

Cluade Shannon derived an analytical formula for the capacity of communication channels. The capacity of a channel in bits per second is given by

$$C = B \log_2(1 + SNR), \tag{4.9}$$

where $B$ is the channel bandwidth, and $SNR$ is the signal-to-noise ratio at the receiver. Shannon's formula gives only a theoretical estimate and assumes a channel without shadowing, fading, and intersymbol interference effects. For wired networks, Shannon's formula gives a good estimate of the maximum achievable data rates. For wireless channels, the achievable data rate is much lower than the one suggested by Shannon's formula. The reason is that the channel characteristics vary with time, owing to shadowing, fading, and intersymbol interference.

### 4.3.4 Channel Coding

*Channel coding* is a mechanism used to make channels immune to noise and to correct errors introduced by the channel. This process involves adding some redundant bits to the transmitted information. These redundant bits can be used for error detection and correction. The use of channel coding can eliminate the need for retransmissions when channel-errors occur. The redundant bits caused can be used to correct the errors and thereby reduce the transmit power and achieve a lower BER.

*Forward error correction* (FEC) is a commonly used scheme for channel coding. FEC schemes normally increase the signal bandwidth and lower the data rate. The *automatic repeat request* (ARQ) scheme explained in previous chapters is normally used along with FEC, as FEC is not sufficient for implementing channel coding. *Turbo codes* have also been successful in achieving data rates near Shannon's capacity. Turbo codes, however, are very complex and have large delays.

### 4.3.5 Flat-Fading Countermeasures

The common techniques used to combat flat fading are *diversity*, *coding and interleaving*, and *adaptive modulation*. With *diversity* multiple independent fading paths are

combined at the receiver to reduce power variations. These independent fading paths can be obtained by separating the signal in time, frequency, or space. Space diversity is one of the most commonly used and effective diversity techniques. An antenna array is used to achieve independent fading paths. Antenna elements in the array are spaced at least one-half wavelength apart.

*Coding and interleaving* is another technique used to counter flat fading. In general, flat fading causes errors to occur in bursts. With coding and interleaving, these burst errors are spread over multiple code words. The adjacent bits from a single code word are spread among other code words to reduce the burst of errors, because burst errors affect adjacent bits. The code words passed to the decoder of the interleaving process contain at most one bit error. FEC channel coding can be used to correct these errors.

*Adaptive modulation* schemes adjust to channel variations. The transmission scheme adapts to the varying channel conditions, based on an estimate that is sent back to the transmitter. The data rate, transmit power, and coding scheme are tailored, based on the received channel estimate. The channel estimate varies, depending on the amount of flat fading. These adaptive schemes help reduce BER and increase efficiency. The adaptive schemes do not function properly if a channel cannot be estimated or if the channel characteristics change very rapidly. It should be noted that the feedback scheme for conveying the channel estimate to the transmitter requires additional bandwidth.

### 4.3.6 Intersymbol Interference Countermeasures

The techniques used to combat *intersymbol interference* (ISI) can be classified into signal-processing techniques and antenna solutions. The signal-processing techniques, which attempt to compensate for ISI or reduce the influence of ISI on the transmitted signal, include equalization, multicarrier modulation, and spread-spectrum techniques. The antenna solutions attempt to reduce ISI by reducing the delay between the multipath components and include directive beams and smart antennas.

The equalization method compensates for ISI at the receiver through channel inversion. The received signal is passed through a linear filter with inverse frequency response, making ISI zero. The noise has to be reduced before passing the signal through the inverse filter. This is done by a linear equalizer called the minimum mean square equalizer. Given a large variation in the channel frequency response, nonlinear *decision-feedback equalizer* (DFE) is used. DFE uses the ISI information from the previously detected symbols to achieve equalization.

DFE is more complex and achieves a much lower BER. Other equalization techniques are the maximum-likelihood sequence and turbo equalization. These schemes

perform better than DFE but are much more complex. The equalizer techniques require an accurate channel estimate to compensate correctly for ISI. As a result, equalizer techniques may not work well for channels in which the characteristics change rapidly.

Multicarrier modulation is another technique used to reduce the effect of ISI. The transmission bandwidth is divided into a number of narrow slots called subchannels. The message signal containing the information to be transmitted is also divided into an equal number of slots. Each of these slots is modulated on one of the subchannels. The resulting sequence is transmitted in parallel. The subchannel bandwidth is maintained less than the coherent bandwidth of the channel. This results in a flat fading instead of a frequency-selective fading in each channel, thereby eliminating ISI. The subchannels can be either nonoverlapping or overlapping. The overlapping subchannels are referred to as *orthogonal frequency division multiplexing* (OFDM). This technique improves the spectral efficiency but results in a greater frequency selective fading, thereby decreasing the signal-to-noise ratio.

### 4.3.7 Orthogonal Frequency Division Multiplexing (OFDM)

In *orthogonal frequency division multiplexing* (OFDM), transmitters generate both the carrier and the data signal simultaneously. OFDM is not a multiple-access technique, as there is no common medium to be shared. The entire bandwidth is occupied by a single source of data. Instead of being transmitted serially, data is transmitted in parallel over a group of subcarriers. Since the carriers are orthogonal to one another, the nulls of one carrier coincide with the peak of another subcarrier, resulting in the possibility of extracting the subcarrier of interest. Contrary to the traditional FDM technique, the spectrum of channels in OFDM significantly overlap.

The process of digital signal generation used in OFDM is based on inverse *fast Fourier transform* (FFT) (see Figure 4.3). A *serial-to-parallel converter* (S/P) converts the serial bits to be transmitted into parallel format. The number of subcarriers and the type of digital communication technique used determine the typical number of bits in parallel. Thus, the incoming data is divided into a large number of carriers. Then *map* and *demap* act as digital modulator and demodulator, respectively. Typically, a *quadrature amplitude modulation* (QAM) or *quadrature phase shift keying* (QPSK) is used as modulator.

The heart of this technique is an inverse *fast Fourier transform* (FFT), in which a carrier frequency is generated based on the location of the stored value. This produces a set of time-domain samples. At the receiver, individual subchannels can be completely separated by FFT only when there is no intersymbol interference in an *add cyclic prefix*

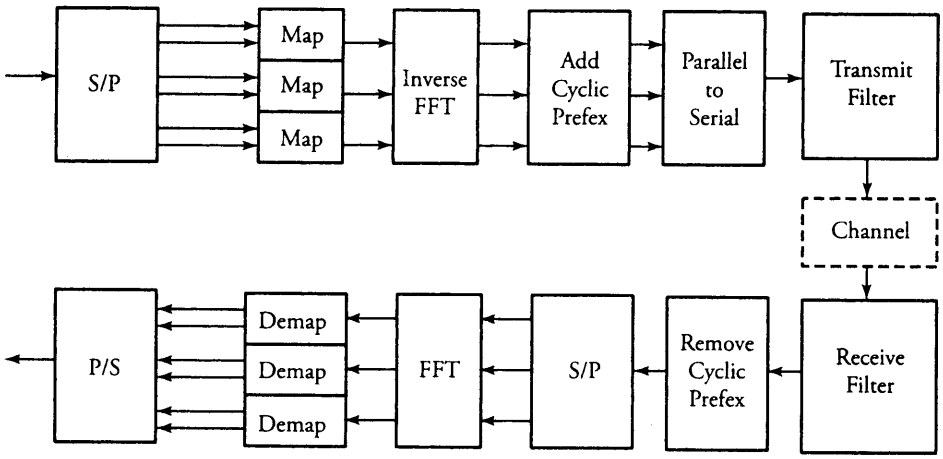


**Figure 4.3** A block diagram of the OFDM technique

acting as a band guard. Note that as the signal travels through the medium, the signal arrives at the receiver at different instances, owing to multipath propagation, resulting in a delay spread leading to ISI. A simple solution to overcome ISI is to widen the symbol duration. This can be achieved by increasing the number of carriers, causing the distortion to become insignificant.

At the receiver, the time waveform is digitized and converted back to a symbol, using FFT. The incoming carrier signal is tracked coherently and sampled in order to be sent to FFT. The time-domain samples are needed at FFT in order to extract the amplitude and phase of the signals. Depending on the amplitude and phase extracted over one symbol time, the frequency-domain representation of the signals obtained. The results are demapped into their original bitstreams, depending on the digital demodulator applied. OFDM signal reception involves a challenging task of time-frequency domains, sampling, and clock synchronization, as well as channel estimations.

## 4.4 Methods of Channel Access on Links

Voice and video applications that run on wireless networks could require continuous transmission, requiring dedicated allocation of available resources for that application. The sharing of the available bandwidth among applications requiring dedicated resources is called *multiple access*. But most wireless applications involve transmission of random bursty data, requiring some form of random channel allocation, which does

not guarantee resource availability. *Multiple-access* techniques assign bandwidth to users by allocating a portion of available spectrum to each independent user.

### 4.4.1 Frequency-Division Multiple Access

In *frequency-division multiple access* (FDMA), the available bandwidth is divided into nonoverlapping, or orthogonal, slots. In other words, each user is assigned a portion of the channel spectrum. FDMA is the simplest multiple-access mechanism that supports multiple users.

### 4.4.2 Time-Division Multiple Access

In *time-division multiple access* (TDMA),each user is assigned a time slot for transmitting. These time slots are nonoverlapping. TDMA techniques are more complex, as they require synchronization in timing among the users. TDMA is also affected by intersymbol interference because of channel distortions, such as multipath delay effects. TDMA divides each channel into orthogonal slots and hence limits the number of users, based on the available bandwidth. TDMA places a hard limit on the number of supported users and bandwidth available for each user. A practical version of TDMA is the *random-access technique* and is mainly used in local area networks.

#### Random Access Techniques

Most wireless networks carry traffic in a bursty form. The dedicated resource allocation schemes, such as multiple-access techniques, prove to be inefficient for some types of systems under bursty traffic. With *random-access* schemes, channels are accessed at random. *Aloha-based* and *reservation-based* protocols are two well-known random-access techniques that require packets to be acknowledged. Distortions in the wireless channel of these schemes, however, may result in loss or delay of acknowledgments. In such cases, a packet retransmission is required, which in turn makes the process inefficient. One solution to this problem would be to use smarter link-layer techniques for the acknowledgment packets to increase their reliability. Common objectives of performing channel access are as follows.

- To minimize interference from other users, a transmitter listens before any transmission.
- To give fair access of the spectrum to all other users, a transmitter transmits for only a certain period of time.
- To minimize transmitter power, the same frequency could be reused in farther areas.

In the basic Aloha scheme, each transmitter sends data packets whenever it has data available to send. This naturally leads to a large number of collisions, and hence a number of data packets have to be retransmitted. Hence, the effective throughput of the Aloha channel is very low because the probability of packet collisions is high. The slotted Aloha scheme was developed to deal with the collision problem. In slotted Aloha, the time is divided into slots, and packet transmission is restricted to these time slots. Thus, the number of collisions is reduced significantly. The throughput with slotted Aloha is double that with basic Aloha. Spread-spectrum techniques are used in combination with Aloha to support a large number of users.

Collision detection and carrier sensing are very difficult in a wireless environment. Shadow-fading effects impair collision detection, as objects obstruct the direct signal path between users. This difficulty of detecting collisions in a wireless environment is often referred to as the *hidden-terminal problem*. Path loss and shadow-fading effects result in signals being hidden between users. Thus, collision-avoidance schemes are normally used in wireless networks, especially in wireless LANs. In a collision-avoidance scheme, the receiver sends a busy tone on receiving a packet. This busy tone is broadcast to all the nearby transmitters. A transmitter that receives a busy tone from any receiver refrains from transmitting. Once the busy tone ends, the transmitter waits for a random amount of time before sending packets. This random back-off scheme is used to prevent all transmitters from transmitting at the same time when the busy signal ends. The collision-avoidance schemes help reduce the collisions in Aloha channels and thus significantly improve the throughput of Aloha.

*Reservation-based schemes* assign channel to users on demand. The effective channel bandwidth is divided between the data channel and the reservation channel. Users reserve channel bandwidth on the reservation channel and send the data packets on the data channel. Users send small packets along the reservation channel, requesting access to the data channel. If a data channel is available, the request is accepted, and a message is sent to the user. Thus, an overhead in reservation-based schemes is the assignment of the data channel. But these data channels are assigned only on demand. For networks on which only small messages are exchanged, the overhead may be tolerable. Also, when the traffic in the network increases rapidly, the reservation channel may get congested with request messages.

The *packet-reservation multiple-access* (PRMA) scheme combines the benefits of the Aloha and the reservation-based schemes. In PRMA, time is slotted and organized into frames, with $N$ time slots per frame. A host that has data to transmit competes for an available time slot in each frame. Once a host successfully transmits a packet in a time slot, the slot is reserved for the user in each subsequent frame until the user has no

more packets to transmit. When the user stops transmitting, the reservation is revoked, and the user has to compete for a time slot to send more packets. PRMA is used in multimedia applications.

### 4.4.3 Code-Division Multiple Access

In *code-division multiple access* (CDMA),users use both time and bandwidth simultaneously, modulated by spreading codes. Spreading codes can be either orthogonal (nonoverlapping) or semiorthogonal (overlapping). Orthogonal spreading codes make it possible to recover the signal at the receiver without any interference from other users. But orthogonal spreading codes place a hard limit on the number of supported users, such as FDMA and TDMA. Semiorthogonal spreading codes involve some interferences from other users at the receiver side. The fundamental superiority of CDMA over other channel-access method lies in the use of the *spread-spectrum technique*.

#### Spread-Spectrum Technique

The *spread-spectrum technique* involves spreading frequencies of a transmitted signal over a wider range. This technique reduces flat fading and intersymbol interference. The message signal is modulated by a *pseudonoise signal*, which encompasses a wider bandwidth. Hence, the resultant transmission signal obtains a much larger bandwidth.

Spread-spectrum techniques can be implemented in two ways. In the first one, *direct sequence*, the message signal is Exclusive-ORed, with the pseudonoise sequence thereby spreading the frequency range. The second technique, *frequency hopping*, involves using the pseudonoise sequence to transmit over a range of frequencies. Frequency hopping is formed based on the random pseudonoise sequence.

#### Rake Receiver

The *rake receiver*, shown in Figure 4.4, is used in a CDMA system where multipath effects are common. The binary data to be transmitted is first Exclusive-ORed with the transmitter's chipping code to spread the frequency range of the transmitted signal. The signal is then modulated for transmission over the wireless medium. The multipath effects in the wireless medium result in multiple copies of the signal, each with different delays of $t_1$, $t_2$, and $t_3$ and with different attenuations of $\alpha_1$, $\alpha_2$, and $\alpha_3$. The receiver demodulates the combined signal and then introduces a variable delay for each signal. Signals are then combined with different weighing factors—$\beta_1$, $\beta_2$, and $\beta_3$—to give the resultant signal with reduced multipath effects.

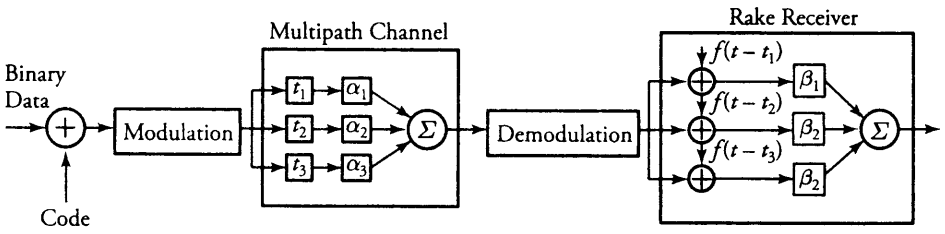


**Figure 4.4** The rake receiver at the heart of CDMA

Semiorthogonal CDMA is the most complex type of multiple-access scheme. But in this technique, the mobile units located far from the receiver experience high interference from other users and hence poor performance. Some power-control schemes are used to mitigate this problem by equalization. The semiorthogonal schemes have the advantage that they do not place any hard limit on the number of users supported. But owing to the semiorthogonal codes, the interference from other users increases as the number of users becomes large. However, the interference can be reduced by using steering antennas, interference equalization, and multiuser detection techniques.

In CDMA, the available frequency bandwidth for each cell is divided in half: one for forward transmission between the base station to the mobile unit and the other part for reverse transmission from the mobile unit to the base station. The transmission technique used is called *direct-sequence spread spectrum* (DSSS). Orthogonal chipping codes are used to increase the data rates and to support multiple users. The transmitted signal also has an increased bandwidth. Using CDMA for cellular systems has several advantages:

- *Diversity in frequency*. In CDMA, the transmitted signal occupies a wider range of frequencies. Therefore, the transmitted signal is not greatly affected by noise and selective fading.
- *Multipath effects*. The orthogonal chipping codes used in CDMA have low cross-correlation and autocorrelation. Hence, multipath signals delayed by more than one chip interval do not interfere with the dominant signal.
- *Privacy*. Since DSSS techniques use pseudorandom sequences, privacy is ensured.
- *Scalability*. FDMA or TDMA systems support only a fixed number of users. CDMA can support a larger number of users with an acceptable amount of degradation in performance. The error rate increases gradually as the number of users becomes larger.

CDMA also has certain disadvantages. In CDMA, the spreading sequences of different users is not orthogonal, and there is some overlap, which results in some cross-correlation, resulting is self-jamming. Also, signals, being at a greater distance from the receiver, experience significant attenuation compared to signals close to the receiver. Thus, signal strength is weak for remote mobile units.

### 4.4.4 Space-Division Multiple Access

The three multiple-access techniques FDMA, TDMA, and CDMA are based on *isotropical antennas*. Recall that an isotropical antenna operates essentially in a uniform manner in all directions. Another method of multiple access in wireless systems is *space-division multiple access* (SDMA), which uses smart antennas. At one end of communication system, a directional antenna, typically known as a smart antenna, can focus directly on the other end of the system. This technique offers a number of advantages, such as reduction of transmission power, reduced amount of interference owing to reduced transmission power, and the strong signal received by the receiver, owing to the high-gain antenna.

### 4.4.5 Hybrid Multiple-Access Techniques

An effective multiple-access scheme needs to be carefully chosen on the basis of application requirements. Practical wireless systems normally use two or more multiple-access techniques. This strategy provides a reasonable growth plan and compatibility with existing systems. Multiple-access methods can also be combined to better serve certain applications. The two most commonly used hybrid schemes are FDMA/TDMA and FDMA/CDMA. Other forms of CDMA are so-called W-CDMA and TD-CDMA. W-CDMA provides higher data rates and uses the spectrum in an efficient manner. TD-CDMA combines W-CDMA and TDMA.

## 4.5 Error Detection and Correction

Error sources are present when data is transmitted over a medium. Even if all possible error-reducing measures are used during the transmission, an error invariably creeps in and begins to disrupt data transmission. Any computer or communication network must deliver accurate messages.

Error detection is applied mostly in the data-link layer but is also performed in other layers. In some cases, the transport layer includes some sort of error-detection scheme. When a packet arrives at the destination, the destination may extract an error-checking

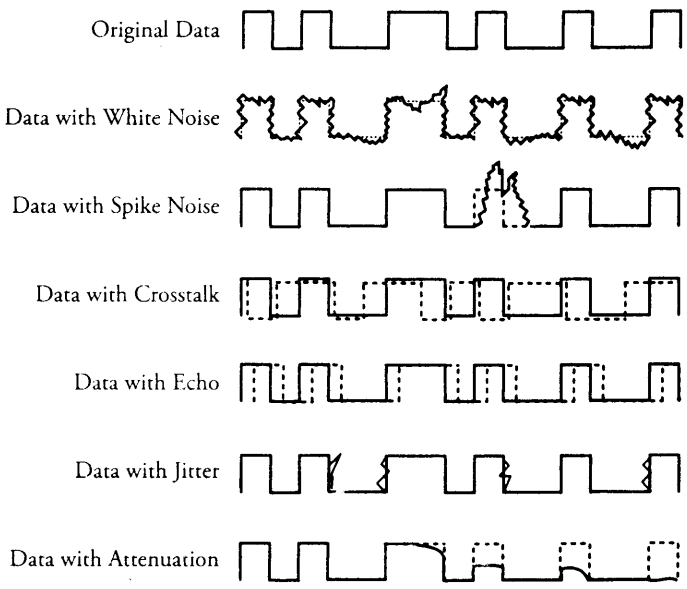


**Figure 4.5** Common forms of data errors at the data-link level

code from the transport header and perform error detection. Sometimes, network-layer protocols apply an error-detection code in the network-layer header. In this case, the error detection is performed only on the IP header, not on the data field. At the application layer, some type of error check, such as detecting lost packets, may also be possible. But the most common place to have errors is still the data-link layer. Possible and common forms of errors at this level are described here and are shown in Figure 4.5.

- *White*, or *Gaussian*, *noise* is continuous and is dependent on the temperature of the medium. White noise might change the content of data, as seen in the figure. White noise can be removed by passing the noisy signal through a set of filters.
- *Spike noise* is not continuous but may completely obliterate the data, so that it cannot be recovered.
- *Cross-talk* is a coupling action between two active links. Coupling can be electrical, as between two sets of twisted-pair wire, or electromagnetic, as when unwanted signals are picked up by an antenna.
- *Echo* is the reflecting impact of a transmitted signal. A signal can hit the end of a cable and bounce back through the wire, interfering with the original signal. This error occurs in bus-type LANs. A one-directional filter, known as an *echo canceler*, can be attached to a link to eliminate echo.

- *Jitter* is a timing irregularity that shows up at the rises and falls of a signal, causing errors. Jitter can result from electromagnetic interference or cross talk and can be reduced by proper system shielding.
- *Bit attenuation* is the loss of a bit's strength as it travels though a medium. This type of error can be eliminated with the use of amplifiers and repeaters for digital systems.

No link is immune to errors. Twisted-pair copper-based media are plagued by many types of interference and noise. Satellite, microwave, and radio networks are also prone to noise, interference and cross talk. Fiber-optic cable too may receive errors, although the probability is very low.

### 4.5.1 Error Detection Methods

Most networking equipment at the data-link layer inserts some type of error-detection code. When a frame arrives at the next hop in the transmission sequence, the receiving hop extracts the error-detection code and applies it to the frame. When an error is detected, the message is normally discarded. In this case, the sender of the erroneous message is notified, and the message is sent again. However, in real-time applications, it is not possible to resend messages. The most common approaches to error detection are

- Parity check
- Cyclic redundancy check (CRC)

The *parity check* method involves counting all the 1 bits in the data and adding one extra bit, called the *parity bit*. This makes the total number of 1 bits even (even parity) or odd (odd parity). The parity-check method is the simplest error-detection technique but is not effective. The *cyclic redundancy check* (CRC) method is one of the most elaborate and practical techniques but is more complex, adding 8 to 32 check bits of error-detection code to a block of data. Our emphasis is CRC.

At this point, we need to clarify that the *Internet checksum* is another error-detection method, though it is used at the network and transport layers and is discussed in Chapters 7 and 8.

### 4.5.2 Cyclic Redundancy Check (CRC) Algorithm

The *cyclic redundancy check* (CRC) method provides smart error checking and has been adopted in most computer and communication systems. Figure 4.6 shows error detection and correction on links, using CRC for a transmitter.

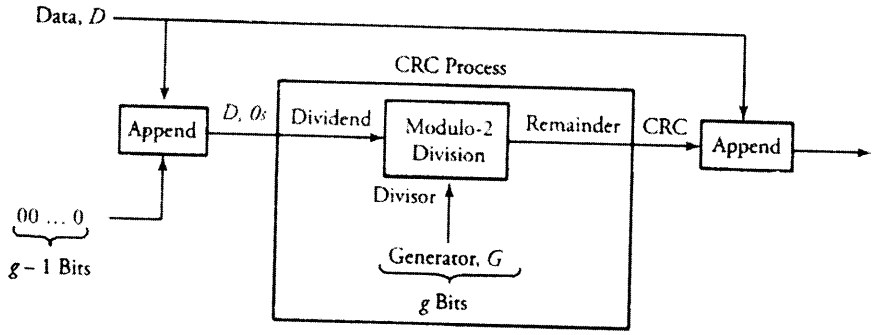


**Figure 4.6** Error detection on links using the CRC method at a transmitter

In any system, a standard and common value between transmitters and receivers is adopted for error processing. This $g$-bit-long value, known as a checking *generator*, is denoted by $G$. At the transmitter, a partial or entire packet or frame is treated as a block of data, and each block is processed individually. The CRC algorithm at the transmitter part can be summarized as follows.

### Begin CRC Algorithm at Transmitter

1. A string of $g - 1$ zero bits is appended to the incoming data, $D$. We call this new block $D$,0s.
2. $D$,0s as a dividend is divided by the generator $G$ acting as the divisor. The division is of type *modulo*-2.
3. The quotient of this division is discarded, but the remainder is called CRC.
4. The CRC value is appended to the data, producing $D$,CRC. ■

At the other end point of the communication system, the receiver receives the value of $D$,CRC and performs the following algorithm to detect errors, as shown in Figure 4.7.

### Begin CRC Algorithm at Receiver

1. $D$,CRC, as a dividend by the same generator $G$ acting as the divisor used by the transmitter. The division is of type *modulo*-2.
2. The quotient of this division is discarded, but if the remainder is 0, the receiver knows that the data has no errors; otherwise, the data is not accepted, as it contains one or more errors. ■

The modulo-2 division arithmetic is very simple. A modulo-2 division function is done without carries in *addition* or borrows in *subtractions*. Interestingly, the module-2 division function performs exactly like the Exclusive-OR logic. For example,

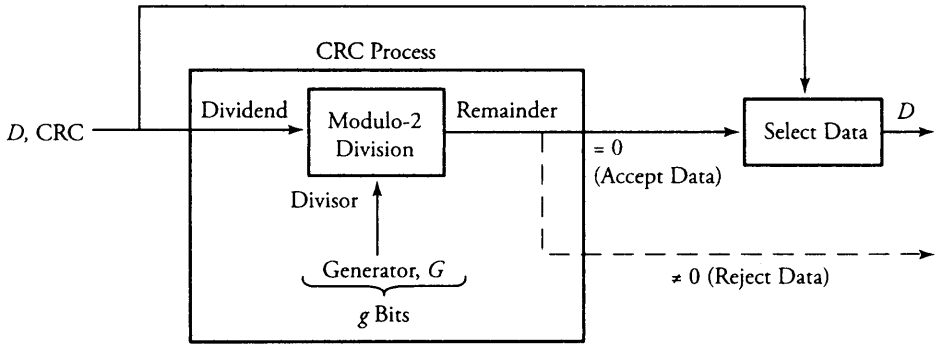


**Figure 4.7** Error detection on links, using CRC at a receiver

with modulo-2 arithmetic, we get $1 + 1 = 0$ and $0 - 1 = 1$. Equivalently, with logic Exclusive-OR: $1 \oplus 1 = 0$, and $0 \oplus 1 = 1$.

**Example.** Assume that 1010111 as a block of data ($D$) is going to be transmitted using the CRC error-checking method. Suppose that the common value of the generator, $G$, is 10010. Produce the final value that the transmitter sends on the link ($D$,CRC), and show the detail of the error-detection process at the receiver.

***Solution.*** At the transmitter, clearly, the number of 0s needed to be appended to $D$ is four ($g - 1 = 4$), since the generator has 5 bits ($g = 5$). Figure 4.8 (a) shows the details of the CRC process at the transmitter side. Since $D$ = 1010111, $D$,0s = 10101110000, the dividend. The divisor is $G$ = 10010. Using modulo-2 arithmetic, the quotient turns out to be 1011100, and the remainder is CRC = 1000. Therefore, the transmitter transmits $D$,CRC = 1010111,1000. At the receiver, as shown in Figure 4.8 (b), $D$,CRC = 1010111,1000 is treated as the dividend and is divided by the same divisor, $G$ = 10010. Since the remainder in this case is 0, the receiver learns that there is no error in the data and can extract the data.

The CRC algorithms are fairly straightforward. Consider again the example. A fact from the modulo-2 arithmetic states that the remainder is always ($g - 1$) bits long; therefore, for this example, the remainder is 4 bits long. Hence, if we make sure that $g - 1$ additional 0s, or four 0s in the example, are at the end of the dividend, the receiver can perform an identical arithmetic in terms of size of dividend. If the transmitter produces a remainder, let's say 1,000, the addition of this value to the same data can indeed result in 0 remainder, provided that the data is the same data used in the transmitter. Therefore, if there is any error during transmission, the remainder may not become 0 at the receiver, giving a notion of error.

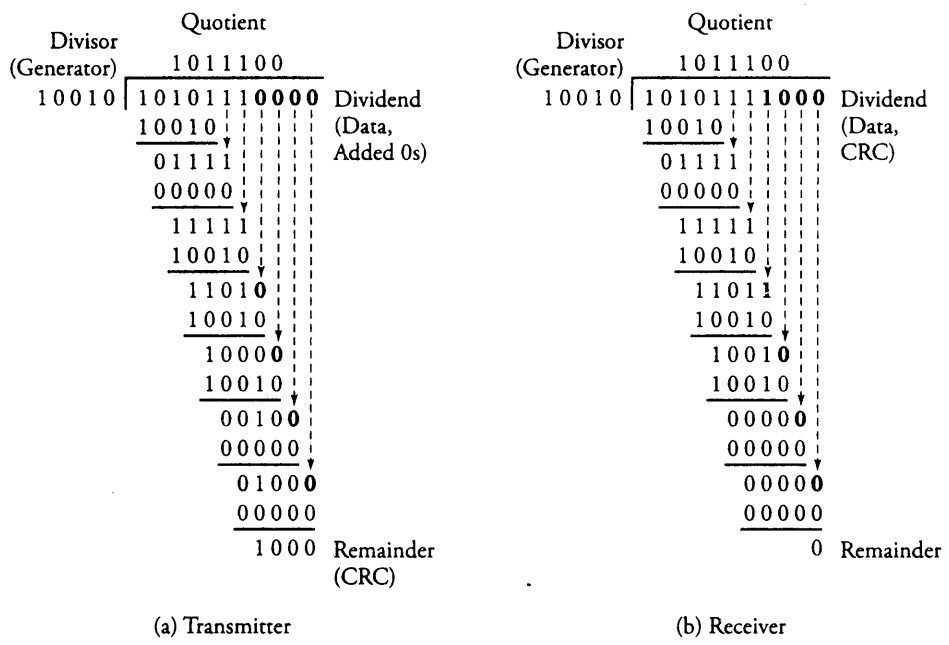


**Figure 4.8** Modulo-2 division for the CRC process shown for a transmitter and a receiver

### Equivalent Polynomial Interpretation

The preceeding analogy can be restated such that the CRC error-detection method treats the data to be transmitted as a polynomial. In general, consider the bit string $a_{n-1}a_{n-2}a_{n-3}\cdots a_0$, which forms a generic polynomial:

$$a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + a_{n-3}x^{n-3} + \cdots + a_0x^0,$$

where $a_i$ can be 0 or 1. In other words, when a data bit is 1, the corresponding polynomial term is included. For example, the bit string $D = 1010111$ produces the string $a_6a_5a_4a_3a_2a_1a_0 = 1010111$, which is interpreted as

$$x^6 + x^4 + x^2 + x^1 + x^0.$$

The *generator* value, acting as the divisor, is known as the *generating polynomial* in this case. Some well-known and widespread industry-approved generating polynomials—

common divisor between transmitters and receivers—used to create the cyclic checksum remainder are:

CRC-8 for ATM: $x^8 + x^2 + x + 1$
CRC-12: $x^{12} + x^{11} + x^3 + x^2 + x + 1$
CRC-16: $x^{16} + x^{15} + x^2 + 1$
CRC-CCITT: $x^{16} + x^{15} + x^5 + 1$
CRC-32 used in IEEE 802:

$$x^{32} + x^{26} + x^{23} + x^{22} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x + 1$$

Note that the polynomial interpretation is simply a convenient method of explaining the CRC algorithm. In practice, the transmitter and the receiver perform divisions in bits, as described earlier.

### Effectiveness of CRC

The CRC method is pretty goof-proof. However, an analysis is needed to answer whether the receiver is always able to detect a damaged frame. Consider the generating polynomial $x^{g-1} + x^{g-2} + \cdots + 1$ with $g$ terms. Apparently, $g - 1$ is the highest power of the generating polynomial. Let $n$ be the length of burst error occurring in a received message. If the size of the error burst is $n < g$, error detection is 100 percent. For all other cases, the terms between $x^{g-1}$ and 1 define which bits are erroneous. Since there are $g - 2$ such terms, there are $2^{g-2}$ possible combinations of erroneous bits. Considering that all combinations can occur with equal probability, there is a chance of $\frac{1}{2^{g-2}}$ that a combination exactly matches the terms of the polynomial. This is the probability of a damaged bit becoming undetected. The probability of catching such error bursts through CRC for all cases is

$$p = \begin{cases} 1 & \text{if } n < g \\ 1 - \left(\frac{1}{2}\right)^{(g-2)} & \text{if } n = g \\ 1 - \left(\frac{1}{2}\right)^{(g-1)} & \text{if } n > g \end{cases}. \tag{4.10}$$

**Example.** Consider a computer communication standard based on CRC-CCITT defined earlier. For this standard, the highest power of the polynomial is $g - 1 = 16$. If the error burst $n$ is less than $g = 17$ bits in length, CRC detects it. Assuming that $n = g = 17$:

$$p = 1 - \left(\frac{1}{2}\right)^{(17-2)} = 0.999969,$$

which is close to 1.

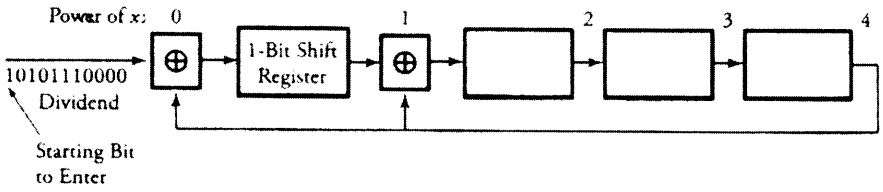


**Figure 4.9** CRC process: The most significant bit enters first.

### Implementation of the CRC Process Unit

Hardware with a combination of software performs the process of division very quickly. An example of the basic hardware used to perform the CRC calculation is shown in Figure 4.9. The hardware includes a simple register that implements the CRC process-generating polynomial $x^4 + x$. Except for the first term ($x^4$), an Exclusive-OR is included for each power of existing term, as shown. Note that the notion of the generator value 10010 is now appearing in the form of hardware shown by a combination of 1-bit shift registers and Exclusive-OR gates. Therefore, we can see from the figure where there is a term in the generating polynomial.

Initially, the registers contain 0s. All data bits of 1010111,**0000**, beginning from the most-significant bit, arrive from the left, and a 1-bit shift register shifts the bits to the right every time a new bit is entered. The rightmost bit in a register feeds back around at select points. At these points, the value of this feedback bit is Exclusive-ORed, with the bits shifting left in the register. Before a bit shifts right, if there is an Exclusive-OR to shift through, the rightmost bit currently stored in the shift register wraps around and is Exclusive-ORed with the moving bit. Once all data bits are fed through, the register's contents must be exactly the same as the remainder indicated in Figure 4.8 (a).

## 4.6 Link-Level Flow Control

Communication systems must use *flow-control techniques* on their transmission links to guarantee that a transmitter does not overwhelm a receiver with data. Several protocols guarantee the control of link flows. Two widely used flow-control protocols are *stop and wait* and *sliding window*.

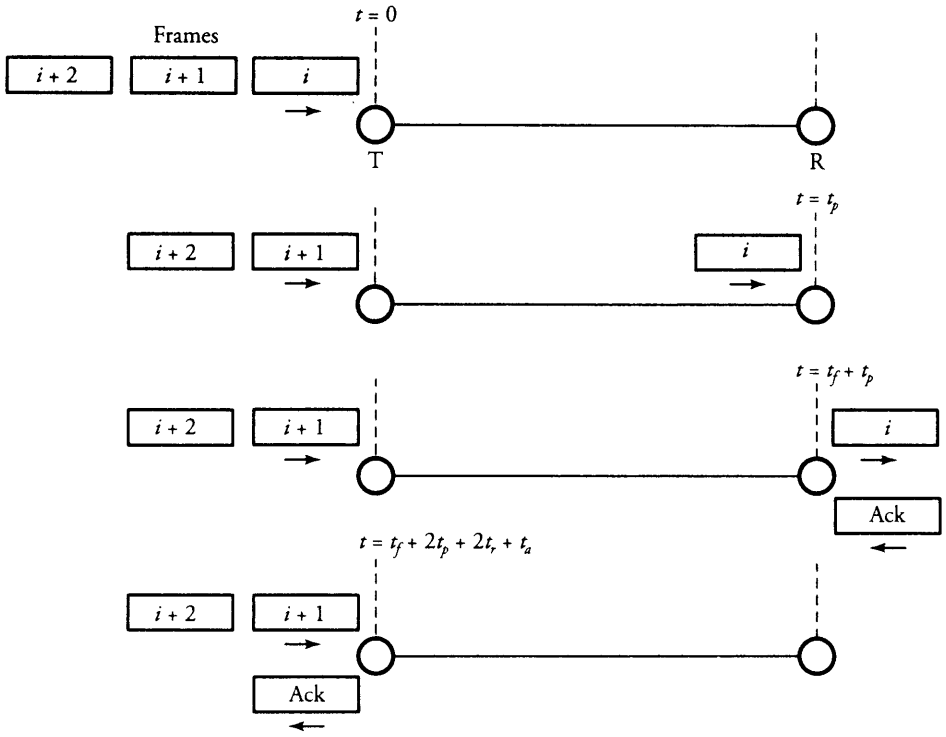


**Figure 4.10** A simple timing chart of a stop-and-wait flow control of data links

## 4.6.1 Stop-and-Wait Flow Control

The *stop-and-wait* protocol is the simplest and the least expensive technique for link-overflow control. The idea behind this protocol is that the transmitter waits for an acknowledgement after transmitting one frame (see Figure 4.10). The essence of this protocol is that if the acknowledgment is not received by the transmitter after a certain agreed period of time, the transmitter retransmits the original frame.

In this figure, we assume two consecutive frames $i$ and $i + 1$. Frame $i$ is ready to enter the link and is transmitted at $t = 0$. Let $t_f$ be the time required to enter all the bits of a frame and $t_p$ the propagation time of the frame between the transmitter (T) and the receiver (R). It takes as long as $t = t_f + t_p$ to transmit a frame. At the arrival of a frame $i$, the receiver processes the frame for as long as $t_r$ and generates an acknowledgment. For the same reason, the acknowledgment packet takes $t = t_a + t_p$

to be received by the transmitter if $t_a$ is assumed to be the time required to enter all the bits of an acknowledgment frame, and it takes $t_r$ for processing it at the receiver. Therefore, the total time to transmit a frame, including acknowledgment processes,

$$t = t_f + 2t_p + 2t_r + t_a. \tag{4.11}$$

Note here that with this technique, the receiver can stop or slow down the flow of data by withholding or delaying acknowledgment. Practically, $t_r$ and $t_a$ are negligible compared to other components of the equation. Thus, this equation can be approximated as

$$t \approx t_f + 2t_p. \tag{4.12}$$

In this equation, $t_f = \ell/r$, where $\ell$ is the length of frame in bits; $r$ is the data rate; and $t_p = d/v$, where $d$ is the length of transmission line, and $v$ is speed of transmission. For wireless and wired transmissions, $v = 3 \times 10^8$ m/s where except for fiber-optic links, $v \approx 2.2 \times 10^8$ m/s, owing to the fact that light travels zigzag over links, and thus overall speed is lower. Therefore, the link efficiency is defined as

$$E_\ell = \frac{t_f}{t} = \frac{1}{1 + 2\left(\frac{t_p}{t_f}\right)}. \tag{4.13}$$

## 4.6.2 Sliding-Window Flow Control

The shortcoming of the stop-and-wait protocol is that only one frame at a time is allowed for transmission. This flow control can be significantly improved by letting multiple frames travel on a transmission link. However, allowing a sequence of frames to be in transit at the same time requires a more sophisticated protocol for the control of data overflow on links. The well-known *sliding-window* protocol is one technique that efficiently controls the flow of frames.

Figure 4.11 shows an example of sliding-window flow control. With this protocol, a transmitter (T) and a receiver (R) agree to form identical-size sequences of frames. Let the size of a sequence be $w$. Thus, a transmitter allocates buffer space for $w$ frames, and the receiver can accept up to $w$ frames. In this figure, $w = 5$. The transmitter can then send up to $w = 5$ frames without waiting for any acknowledgment frames. Each frame in a sequence is labeled by a unique sequence number. For every $k$ frames forming a sequence, the transmitter attaches a sequence-number field to each frame. Therefore, as many as $2^k$ sequence numbers exist.

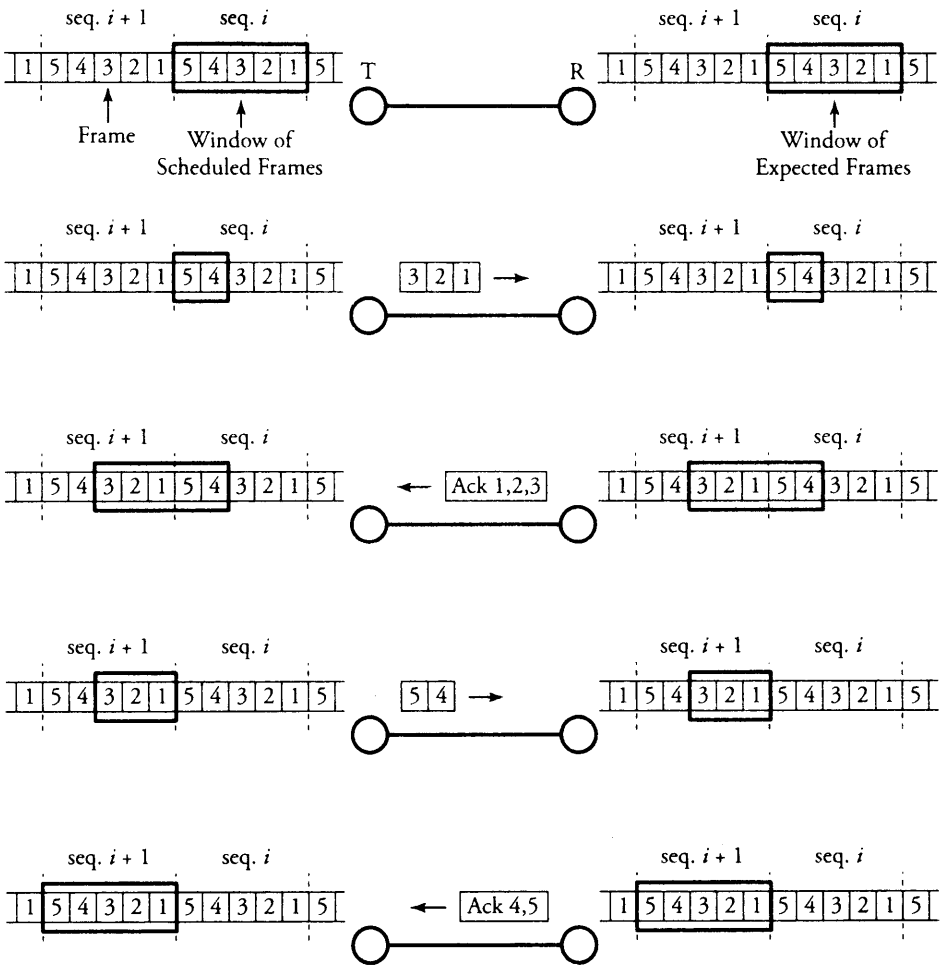


**Figure 4.11** Timing chart of a sliding-window flow control for two sequences of frames

First, a transmitter opens a window of size $w = 5$, as the figure shows. The receiver also opens a window of size $w$ to indicate how many frames it can expect. In the first attempt, let's say that frames 1, 2, and 3 as part of sequence $i$ are transmitted. The transmitter then shrinks its window to $w = 2$ but keeps the copy of these frames in its buffer just in case any of the frames is not received by the receiver. At the receipt of these three frames, the receiver shrinks its expected window to $w = 2$ and acknowledges the receipt of frames by sending an acknowledgment ACK1,2,3 frame to the transmitter.

At the release of ACK1,2,3, the receiver changes its expected window size back to $w = 5$. This acknowledgment also carries information about the sequence number of the next frame expected and informs that the receiver is prepared to receive the next $w$ frames. At the receipt of ACK1,2,3, the transmitter maximizes its window back to $w = 5$, discards the copies of frames 1, 2, and 3, and continues the procedure. In this protocol, the window is imagined to be sliding on coming frames. Similarly, we can derive an expression for this protocol as we did for the stop-and-wait protocol. For the transmission of a frame as the integral portion of $w$ frames sequence, the total time, including all the acknowledgment processes, is obtained using Equation (4.11), with averaging over $w$ and inclusion of $wt_f$ as

$$t = \frac{1}{w}(wt_f + 2t_p + 2t_r + t_a). \tag{4.14}$$

Practically, $t_r$ and $t_a$ are negligible; thus, this equation can be approximated by

$$t \approx t_f + 2\left(\frac{t_p}{w}\right). \tag{4.15}$$

Therefore, link efficiency is expressed as

$$E_\ell = \frac{t_f}{t} = \frac{w}{w + 2\left(\frac{t_p}{t_f}\right)}. \tag{4.16}$$

Link efficiency provides a network designer with a good understanding of the link utilization for network management purposes.

## 4.7 Summary

We started this chapter by discussing wired and wireless transmission media. Data can travel on guided links, such as optical fibers, and unguided links, such as certain types of wireless links. Link capacity is further partitioned into *channels*. Wireless channels have several weaknesses, such as shadow fading, path loss, and interference. Methods of accessing link channels deal with how to mediate access to a shared link so that all users eventually have a chance to transmit their data. We examined frequency-division, time-division, code-division, and space-division multiple-access methods; in most cases, time-division multiple-access methods offer several benefits for channel access in local area networks.

We also looked at methods that determine whether transferred bits are in fact correct or whether they possibly were corrupted in transit. With the *cyclic redundancy check*

(CRC) method, some frames arriving at the destination node contain errors and thus have to be discarded.

Two link-control schemes are *stop and wait* and *sliding window*. In the stop-and-wait method, a sender waits for an acknowledgment after transmitting one frame. This flow-control method is significantly improved in the *sliding window* method, which lets multiple frames travel on a transmission link.

In the next chapter, we use our knowledge of data links from Chapters 2, 3, and 4 to form small local area networks.

## 4.8 Exercises

1. In order to transmit a 500-page book with an average of 1,000 characters per page between places 5,000 km apart, we assume that each character uses 8 bits, that all signals travel at the speed of light, and that no link-control protocol is used.
   (a) How much time is required if a digital voice circuit operating at the speed of 64 kb/s is used?
   (b) How much time is required if a 620 Mb/s fiber-optic transmission system is used?
   (c) Repeat parts (a) and (b) for a library with 2 million volumes of books.
2. Assume that a wireless system with 200 terminals uses TDMA for its channel access. The packet lengths are $T$ in average and are considered short compared with the TDMA long channel length. Compare the efficiency of two strategies: *polling* and CSMA.
3. Design a CRC process unit for the following two standard generators of computer networking:
   (a) CRC-12
   (b) CRC-16
4. For the example presented in the CRC section, we had 1010111 as a block of data *(D)*, and the common value of generator, *G*, 10010, as the divisor.
   (a) Show the dividend and the divisor in polynomial forms.
   (b) Divide the dividend and the divisor in polynomial forms.
   (c) Compare the results of part (b) to its binary form obtained in example.
5. For data $D$ = 1010111,0000, presented in the example of the CRC section, and the common value of generator, $G$ is 10010 as the divisor. Sketch a picture of

Figure 4.9 as many as needed and every time you shift in a bit, show the content of each register. Prove that the final contents of the registers show the value of CRC.

6. Assume that 101011010101111 is a block of data *(D)* to be transmitted using the CRC error-checking method. Suppose that the common value of generator, *G*, is 111010. Using modulo-2 arithmetic.
   (a) Produce the final value that the transmitter sends on the link *(D,*CRC).
   (b) Show the detail of the error-detection process at the receiver.

7. Consider a coaxial transmission link that uses the stop-and-wait protocol requiring a propagation time to transmission time ratio of 10. Data is transmitted at rate 10 Mb/s, using 80-bit frames.
   (a) Calculate the efficiency of this link.
   (b) Find the length of this link.
   (c) Find the propagation time.
   (d) Sketch a plot of link efficiency when the ratio of propagation time to transmission time is reduced to 8, 6, 4, and 2.

8. Consider a 2 Mb/s satellite transmission link through which 800-bit frames are transmitted. The propagation time is 200 ms.
   (a) Find the link efficiency, using the stop-and-wait protocol.
   (b) Find the link efficiency, using the sliding-window protocol if the window size is $w = 6$.

9. Consider the bidirectional control of links with the sliding-window method applied between two routers R2 and R3 (window size $w = 5$) and stop-and-wait control between routers R3 and R4. Assume that the distance between R2 and R3 is 1,800 km and is 800 km between R3 and R4. A total of 1000 data frames with average size of 5,000 bits flow from R2 to R3 at 1 Gb/s rate. Acknowledgment frames are small enough to be ignored in the calculations. All links generate 1 $\mu$s/km propagation delay.
   (a) Determine a condition on the data rate at the output port of R3 toward R4 so that R3 remains congestion-free.
   (b) Find the link efficiency for the R2–R3 link.
   (c) Find the link efficiency for the R3–R4 link.

CHAPTER 5

# Local Area Networks and Networks of LANs

A *local area network* (LAN) is a small interconnection infrastructure that typically uses a shared transmission medium. Because of such factors as the volume of traffic, the level of security, and cost, the network structure in a local area network can be significantly different from that for a wide area network. This chapter focuses on the fundamentals of local area networks and describes the *internetworking* concept at the LAN level. major topics are as follows:

- *Basic LAN topology*
- *LAN protocols*
- *MAC and IP addresses*
- *Classification of MAC protocols*
- *Contention-access MAC*
- *Round-robin-access MAC*
- *Network of LANs*

First, we explore some simple topologies of local area networks and see how a LAN is formed. We then extend the discussion of protocols presented in Chapter 2 to LAN protocols, focusing on *medium access control* (MAC) and addressing. We explore two well-known methods of link-access methods: *contention* and *round-robin*.

Another important topic is *internetworking*. Some pointers toward internetworking LANs with repeaters and bridges are provided. The focus of this chapter is primarily on layer 2 of the protocol stack reference model.

## 5.1 LANs and Basic Topologies

A LAN is used for communications in a small community in which resources, such as printers, software, and servers, are shared. Each device connected to a LAN has a unique address. Two or more LANs of the same type can also be connected to forward data frames among multiple users of other local area networks. In LANs, packets are additional headers appended for local routing. These new-looking packets are known as *frames*. Users in a local area network can be interconnected in several ways. The fundamental network topology in LANs can be categorized into *bus*, *ring*, and *star*, as shown in Figure 5.1.

In the *bus* topology, all users are connected to a common transmission medium referred to as a bus. The users are connected to a common bus via a duplex link that allows both uplink and downlink operations, as seen in the figure. The transmission from a user is propagated on the bus in both directions, and all users in the path receive its frame. However, only the destination user copies the frame into its computer; all other users discard the frame.

The *ring* topology comprises of layer 1 and 2 devices such as *repeaters* (see Section 3.3.1). Repeaters are interconnected to form a closed loop, and each user is connected to one repeater, shown in the figure by a smaller circle. When a user transmits a frame, its associated repeater forwards the frame to the ring. The ring is normally unidirectional, so a frame can flow in one direction. During the circulation of the frame in the ring, the destination user copies the frame onto its buffer. Once copied by the destination, the frame continues its circulation until the sender receives it and removes it from the system. To avoid collision, only one user can transmit at a given time.

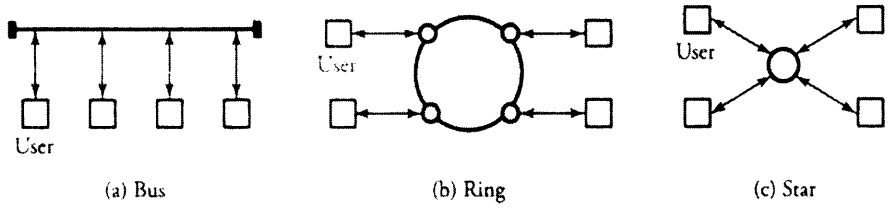


**Figure 5.1** Three fundamental LAN configurations to connect users

In the *star* topology, all users are directly connected to a central user through two unidirectional links: one for uplink and the other for downlink. The central user functions in either broadcast mode or frame-switch mode. In *broadcast mode*, the central user is called a *hub* (see Section 3.3.1). When it receives the frame from a user on the uplink, the hub retransmits the frame to all users on the downlink. Broadcast mode allows only one user to transmit at a time. In *frame-switch mode*, the central user buffers the received frame and retransmits the frame only to the destination.

## 5.2 LAN Protocols

Protocols designed for layers 3 and above are independent of the underlying network topology. Hence, protocols designed for LANs are normally concerned with the data-link layer and the physical layer. Organizations working on LAN standards comply with the specifications of IEEE 802 reference model. The physical layer of a LAN implements such functions as signal transmission and reception, encoding and decoding, and generation and removal of synchronization information. The physical layer also specifies the type of medium used for transmission and the network topology.

Figure 5.2 shows the position of the two LAN sublayers in the overall structure of the protocol stack. The IEEE 802 standard subdivides the *data-link layer* of the protocol model into the *logical-link control* (LLC) layer and the *media access control* (MAC) layer. The LLC layer implements flow and error control apart from providing an interface to the network layer. The MAC layer primarily controls the access to transmission medium and is responsible for framing. LLC has the option of choosing from various types of MAC layers.

### 5.2.1 Logical-Link Layer (LLC)

Data to be transmitted from the higher layers is passed down to the *logical-link layer*, which determines the mechanism for addressing users across the medium. The LLC also

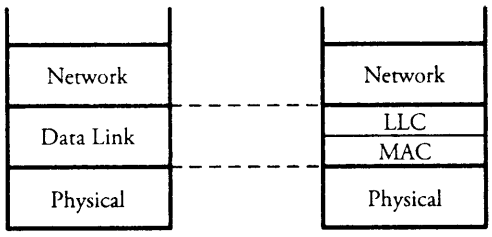


**Figure 5.2** LAN sublayer protocols in the overall structure of the protocol stack

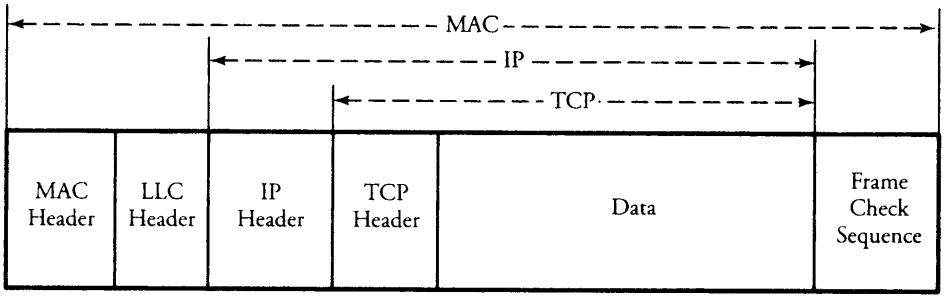


**Figure 5.3** Generic MAC frame format

controls the exchange of data between each two users. The LLC appends its header to form the LLC protocol data unit, which is then sent to the MAC layer, which appends the header and the frame check sequence to create the MAC frame.

### 5.2.2 Medium Access Control (MAC)

A LAN is required to provide sharing access to the transmission medium. To ensure efficient access to a medium, users have to comply with some rules. The MAC protocol manages access to the medium. Figure 5.3 shows a generic MAC frame format within frame formatting for the MAC protocol. The fields of the frame format are as follows.

- *MAC header* gives the MAC control information, such as the MAC address of the destination and the priority level.
- *LLC header* contains the data from the logical-link layer.
- *IP header* specifies the IP header of the original packet.
- *TCP header* specifies the TCP header of the original packet.
- *Frame check sequence* is used for error checking.

The next section provides a detailed discussion on MAC and its interaction with IP addresses.

## 5.3 MAC and IP Addresses

Each node has an IP address. Each node's adapter to its attached link has a link-layer address, which is in fact the MAC *address*. A MAC address is as wide as 6 bytes and is normally shown in hexadecimal notation, such as 00-40-33-25-85-BB. The MAC address is unique for each device and is permanently stored in the adapter's read-only

memory. Consequently, networking manufacturers need to purchase MAC addresses for their products. Unlike an IP address, a MAC address is not hierarchical. The advantage of MAC addressing is that a device may not need to have an IP address in order to communicate with the surrounding devices in its own LAN.

Each node adapter that receives a frame checks whether the MAC address of the frame matches its own MAC address. If the addresses match, the adapter extracts the inner packet and passes it up the protocol stack. In summary, each destination address specified in an IP header is the logical address and is different from the physical or the link-layer address. For a packet from a source host to be delivered successfully to its destination, the host needs to identify both the IP address and the link-layer address. The source uses the *address resolution protocol* (ARP) to find the link-layer address of a destination.

### 5.3.1 Address Resolution Protocol (ARP)

The *Address Resolution Protocol* (ARP) is designed to convert IP addresses to MAC addresses or vice versa. Suppose that a user wants to transmit a packet to its destination. If it does not know the link-layer address of the destination, the sender broadcasts an ARP packet requesting the link-layer address given the IP address. The destination is denoted by its IP address in the ARP request. Only the destination replies with its link-layer address. The sender then stores this address in the local ARP table for its subsequent use. Each networking device, such as a host or a router, has an interface, or *adapter*. Each adapter has a table that keeps the MAC address of each device within the network it is attached to. MAC addresses are listed in the adapter's ARP table.

**Example.** Figure 5.4 shows that LAN1 has several users. A user with IP address 133.176.8.55 and adapter MAC address AB-49-9B-25-B1-66 wants to send a frame within its LAN to user 133.176.8.56 with adapter MAC address 11-40-33-55-A3-57. In this case, original packets are converted to frames in its adapter with the destination address AB-49-9B-25-B1-66. Now suppose that the same sender wants to send frames outside its LAN to a user in LAN3 with IP address 198.34.7.25 connected through a four-port router. But assume that the sender does not know the MAC address of the destination. In this case, the sender must broadcast an ARP packet to all users, but only the destination user replies to the ARP query, providing its adapter MAC address of 33-BA-76-55-A3-BD. This new address is used for the router to forward the message of the sending user to the destination.

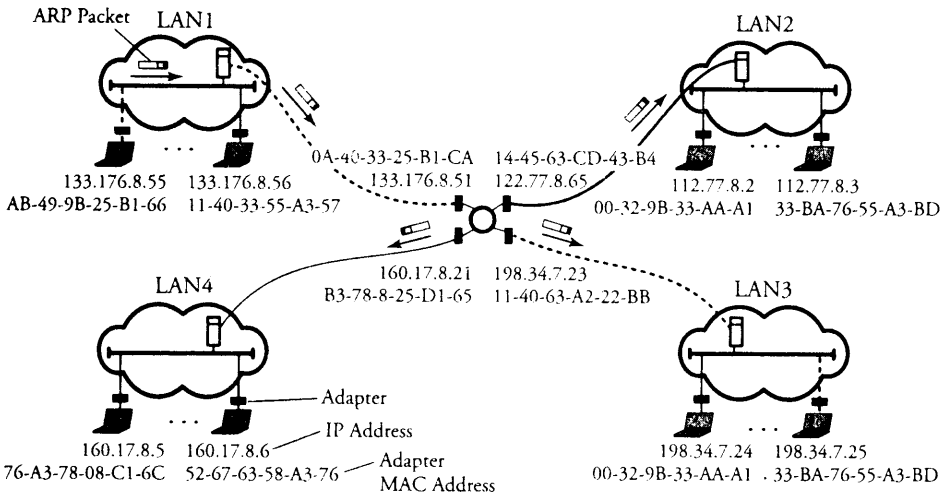


**Figure 5.4** ARP packets and MAC and port adapters

### 5.3.2 Reverse Address Resolution Protocol (RARP)

*Reverse Address Resolution Protocol* (RARP) too is a protocol to find a certain address. But in this case, RARP is used when the link-layer address of the destination is known but not its IP address. The host broadcasts the link-layer address of the destination and requests the IP address. The destination responds by sending the IP address.

## 5.4 Classification of MAC Protocols

MAC protocols can be broadly classified as *centralized* or *distributed* based on the type of network architecture. In the centralized scheme, a central controller controls the operation of the users, and users communicate only with the controller. Users adhere to the transmission schedule specified by the controller. In a distributed network, users talk to each other and dynamically determine the transmission schedule. Centralized schemes are used in applications that require a simple access scheme, QoS, and guaranteed capacity. However, centralized schemes are vulnerable to a single point of failure. Distributed schemes have no single point of overall failure. Yet, coordinating access among devices is a complex process for distributed schemes, and the network cannot provide a QoS guarantee.

MAC protocols can also be characterized as *synchronous* or *asynchronous*. In the synchronous scheme, such as time-division multiplexing and frequency-division mul-

tiplexing, capacity is preassigned to each connection. The synchronous scheme is rarely used in LANs, as users' transmission requirements vary dynamically. Rather, it is optimal to assign capacity to users asynchronously, based on demand.

In terms of access to the shared medium, MAC protocols can be broadly classified into two types:

- *Contention access*, by which each user needing to transmit data must contend to access the medium
- *Round-robin access*, by which each user is given a chance to transmit data in a round-robin fashion

The details of these two protocols are presented in Sections 5.5 and 5.6.

A third category of access method is *reservation-access* MAC. This application-specific method is used mainly for streaming traffic. With this method, as in synchronous time-division multiplexing, time slots are used to access the medium. A user can reserve time slots for transmission in advance. The control mechanism for the reservations can be either centralized or decentralized.

## 5.5 Contention-Access MAC

*Contention-access* MAC is stochastic, more suitable for bursty traffic, whereby the waste of shared-medium bandwidth cannot be tolerated. Unlike the round-robin and reservation schemes, no control is involved in the contention scheme. Rather, each user needing to transmit frames must contend to access the medium. This scheme is simple to implement and is an effective solution for light or moderate traffic.

When a user logs on to a LAN, a channel for the transmission of a frame can be demanded at any random instance, potentially resulting in frame collision. This serious issue can be resolved in a number of ways, as follows:

- *Permanent assignment of one channel to each user*. This method can clearly waste the system bandwidth.
- *Checking users regularly*. The system can poll each user on a regular basis to see whether it has anything to transmit. This method could result in a long delay for larger networks.
- *Random access of a channel*. The system can provide a mechanism whereby a user can access at any time. This method is efficient but faces the collision issue if two or more frames are transmitted at the same time.

Several random-access methods are provided for computer networks. Two commonly used ones are *Aloha* method (see Section 4.4.2) and *Carrier Sense Multiple Access* (CSMA). The CSMA scheme is explained in the next section.

### 5.5.1 Carrier Sense Multiple Access (CSMA)

*Carrier Sense Multiple Access* (CSMA) is a protocol that lets only one user at a time transmit, on a first come, first served basis. A user needing to transmit data first listens to the medium and senses for a carrier on the medium to determine whether other users are transmitting: the *carrier-sense* phase. If the medium is busy, the user has to wait until the medium is idle. The amount of time a user must wait depends on the particular type of the protocol. If no other users transmit data, the user proceeds to transmit its data onto the medium. However, when the medium is busy, a user can follow one of the following three approaches:

1. *Nonpersistent CSMA.* The user waits for a random amount of time after a collision before sensing the channel again. The random delay is used to reduce the collision. However, this scheme uses the transmission channel inefficiently: Even though the transmission is completed, the user rechecks the medium only after expiration of the random delay. The random wait time is normally 512 $g$ bit times, where $g$ is a number drawn randomly.
2. *1-persistent CSMA.* This scheme overcomes the disadvantage of the nonpersistent CSMA by continuing to sense the channel while it is busy. As soon as the medium is idle, the user transmits immediately. In this scheme, a collision occurs if more than one user is waiting to transmit.
3. *p-persistent CSMA.* This scheme is a compromise between the nonpersistent and the 1-persistent methods. When the medium is idle, the user can transmit with a probability $p$. If the medium is busy, the user can transmit for a time equal to the maximum propagation delay. Deciding on an appropriate value of $p$ is crucial for efficient operation of the scheme.

If two or more users simultaneously try to transmit, a collision of frames occurs, and all data is corrupted. In such a case, all corresponding users stop transmitting. Thus, after a collision, all the users involved will start contention, each after a randomly chosen amount of time. After finishing the transmission of data, a user waits for an acknowledgment from the destination user. If the acknowledgment does not arrive, the user retransmits the data.

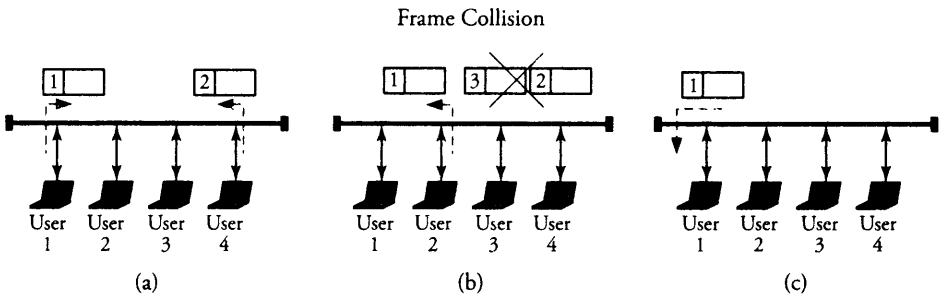


**Figure 5.5** The movement and collision of frames in a contention-access MAC network

The main disadvantage of CSMA when a collision occurs is that other users cannot use the medium until all corrupted frames finish transmission. This problem increases in the case of long frames. However, this issue can be resolved with the use of CSMA/CD, whereby a user listens to the channel while transmitting data. In case of a collision, the transmission is halted, and a jamming signal is transmitted to inform the other users that a collision has occurred. The user enters into *back-off mode* and transmits after the back-off duration if the medium is idle. In Figure 5.5, a frame that leaves user 4 destined for user 2, collides with another frame that leaves user 1 destined for user 3. Immediately after the collision, user 2 finds the medium idle and transmits its frame destined to user 1.

Consider $n$ users to be connected onto a common cable so that when one user transmits a frame while others are silent, all other users sense that frame. When a user starts the transmission, no others start before the user has propagated a signal throughout the cable. This way, the user can finish its frame without collision. The CSMA/CD method can be set up to detect collisions ahead of time. It is quite possible for a user to listen to the cable while transmitting; obviously, if two or more users start to transmit simultaneously, they find a collision in process and cease transmission. That is why this process is called CSMA collision detection (CSMA/CD).

CSMA/CD requires the frame length to be long enough to permit collision detection before the completion of transmission. The maximum time to detect a collision is not greater than twice the end-to-end propagation delay. The process of CSMA/CD is viewed in terms of slots and minislots. Setting minislots is required for a signal to propagate from one end of the cable to the other. Minislots are used in a contention mode. If all users are synchronized in minislots and one user transmits during an empty slot, all the other users pick up the transmitted frame until the frame is transmitted

completely. However, if more than one user transmits during that slot, each transmitting user senses the situation and ceases transmitting.

### Analysis of Frame Delay

Consider once again the bus LAN shown in Figure 5.5. Let $\ell$ be the average distance between any two users. The maximum $\ell$ is the distance between user 1 and user 4, and the minimum $\ell$ is the distance between user 1 and user 2. Let $c$ be the speed of propagation. The average propagation delay of a frame between any two users can be determined by

$$t_p = \frac{\ell}{c}. \tag{5.1}$$

Now, let $f$ be the average frame size in bits and $r$ be the data rate on the channel over the medium. The frame transmission time, $t_r$, can be calculated by

$$t_r = \frac{f}{r}. \tag{5.2}$$

Here, the *utilization* of the LAN bus can be obtained by

$$u = \frac{t_r}{t_r + t_p}. \tag{5.3}$$

### Analysis of Contention

If a total of $n$ users are attached to the medium and $n_a$ of them are active, the probability of a user restraining itself to resend its frame during a time slot is

$$p = \frac{1}{n_a}. \tag{5.4}$$

In general, an empty time slot remains empty, is taken by a user, or undergoes a collision. Apparently, the probability that a user attempts to transmit frames in an empty time slot is

$$p_c = \binom{n_a}{1} p^1(1-p)^{n_a-1} = n_a p(1-p)^{n_a-1}. \tag{5.5}$$

By combining the two Equations (5.4) and (5.5), we obtain

$$p_c = \left(\frac{n_a - 1}{n_a}\right)^{n_a-1}. \tag{5.6}$$

This probability value merges to $\frac{1}{e}$ when $n_a$ approaches a very large number. A different situation is that a frame tries $i$ times in $i$ empty slots to transmit its frame and is unsuccessful owing to collision, but it successfully sends its frame on time $i + 1$. The probability that this situation happens is obviously modeled by a geometric random variable, explained in Appendix C, and is obtained by

$$P_i = P_C(1 - P_C)^i. \tag{5.7}$$

Interestingly, the average number of contentions can be computed by knowing this behavioral model using the expected value explained in Appendix C:

$$\begin{aligned} E[C] &= \sum_{i=1}^{\infty} ip_i = \sum_{i=1}^{\infty} ip_C(1 - p_C)^i \\ &= \frac{1 - p_C}{p_C}. \end{aligned} \tag{5.8}$$

**Analysis of Throughput**

Consider Figure 5.6, and assume that the frame arrivals on the network have a Poisson distribution (see Appendix C for the details of the Poisson model) with an average arrival rate $\lambda$ and a frame duration of $T$ seconds. Based on this model, the probability that there are $k$ frames in a given period $[0, t]$ is obtained from

$$P_X(k) = \frac{(\lambda t)^k e^{-\lambda t}}{k!}. \tag{5.9}$$

We start with frame 2 and let $t_p$ be the total propagation delay between any pair of users. Thus, the probability that a frame is transmitted successfully, $P_t$, is the probability that no additional frame is transmitted during $t_p$ and is expressed by Equation (5.9) when $k = 0$ as

$$P_t = P_X(0) = e^{-\lambda t_p}. \tag{5.10}$$

The delay time caused by the last colliding frame is modeled by a random variable, $Y$. The probability that this last frame is transmitted at or before time $y$ is the probability that no other frames are transmitted in the interval $(y,t_p]$ and is obtained from

$$P[Y \leq y] = e^{-\lambda(t_p - y)}. \tag{5.11}$$

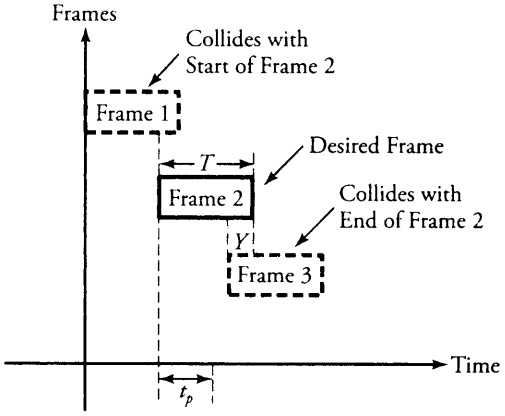


**Figure 5.6** A timing illustration of CSMA/CD

The preceding probability is clearly calculated only for $0 < y < t_p$ and is known as the *cumulative distribution function* (CDF) of the random variable $y$. If this distribution is known, the *probability density function* (PDF), or $f_Y(y)$, can be determined (see Appendix C); thus, the average of time $y$ can be estimated by the expected value of $y$:

$$E[Y] = \int_0^{t_p} y f_Y(y) dy = t_p - \frac{1 - e^{-\lambda t_p}}{\lambda}. \tag{5.12}$$

As seen in Figure 5.6, the average *busy time* of a channel, $t_B$, has three components: frame duration ($T$), propagation delay ($t_p$), and the relative delay of the last colliding frame ($E[Y]$):

$$t_B = T + t_p + E[Y] = T + 2t_p - \frac{1 - e^{-\lambda t_p}}{\lambda}. \tag{5.13}$$

From the property of the Poisson random variable, we calculate the average idle time as

$$t_I = \frac{1}{\lambda}. \tag{5.14}$$

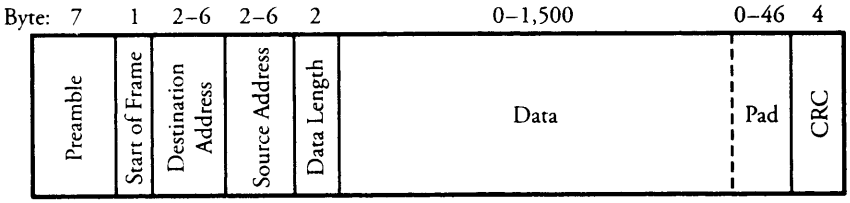


**Figure 5.7** Details of Ethernet IEEE 802.3 LAN frame

The overall throughput of a CSMA/CD channel is defined as the number of frames per time slot and is obtained from

$$\begin{aligned} R &= \frac{P_t}{t_B + t_I} \\ &= \frac{e^{-\lambda t_p}}{\left(T + 2t_p - \frac{1-e^{-\lambda t_p}}{\lambda}\right) + \frac{1}{\lambda}} \\ &= \frac{\lambda e^{-\lambda t_p}}{\lambda(T + 2t_p) + e^{-\lambda t_p}}. \end{aligned} \tag{5.15}$$

Throughput $R$ can be normalized to throughput per frame time, or $R_n$. Practically, $R_n$ is easier to use for the estimation of the system throughput.

## 5.5.2 Ethernet LAN: IEEE 802.3 Standard

The IEEE 802.3 standards committee developed a widely used LAN standard called *Ethernet*, which covers both the MAC layer and the physical layer. The IEEE 802.3 standard uses CSMA for controlling media access and the *1-persistent* algorithm explained earlier, although the lost time owing to collisions is very small. Also, IEEE 802.3 uses a back-off scheme known as *binary exponential backoff*. The use of random backoff minimizes subsequent collisions. This back-off scheme requires a random delay to be doubled after each retransmission. The user drops the frame after 16 retries. The combination of the 1-persistent scheme and binary exponential backoff results in an efficient scheme. A brief description of the frame fields follows and is shown in Figure 5.7.

- *Preamble* is 7 bytes and consists of a pattern of alternating 0s and 1s. This field is used to provide bit synchronization.

- *Start of frame* consists of a 10101011 pattern and indicates the start of the frame to the receiver.
- *Destination address* specifies the destination MAC address.
- *Source address* specifies the source MAC address.
- *Length/Type* specifies the frame size, in bytes. The maximum Ethernet frame size is 1,518 bytes.
- *LLC data* is data from the LLC layer.
- *Pad* is used to increase the frame length to the value required for collision detection to work.
- *Frame check sequence* is 32-bit CRC for error checking (see Section 4.5.2).

The Ethernet versions have different data rates. Version 1000BaseSX, carrying 1 Gb/s, and 10GBase-T, carrying 10 Gb/s, hold the most promise for the future of high-speed LAN development.

## 5.6 Round-Robin-Access MAC

Unlike contention-access MAC, the *round-robin-access* scheme is deterministic, and there is no random allocation of a time slot to a frame. Although this scheme is not as popular as the contention-access LANs, some practical applications are associated with this scheme. Round-robin-access MAC is effective when most users have large amounts of data to transmit, such as in stream traffic.

Each user is given a chance to transmit data in a round-robin fashion. Each user may transmit data; if it has no data to transmit, the user passes its turn to the next user. Round-robin access can be implemented in a couple of ways. One method is known as the *token-ring access*.

### 5.6.1 Token-Ring Access Protocol

The *token-ring* configuration (see Figure 5.8) is based on the round-robin-access MAC. Token-ring passing is a method used for accessing the medium. The ring comprises repeaters interconnected with unidirectional links to form a closed loop. Each user is connected to a repeater. Repeaters perform data insertion, data reception, and data removal. A *token* is a small frame that is injected into the ring and circulated through the ring. Normally, one user is responsible for this task. Once a new token is circulated through the ring, the user needing to transmit captures the token and then starts transmitting data.

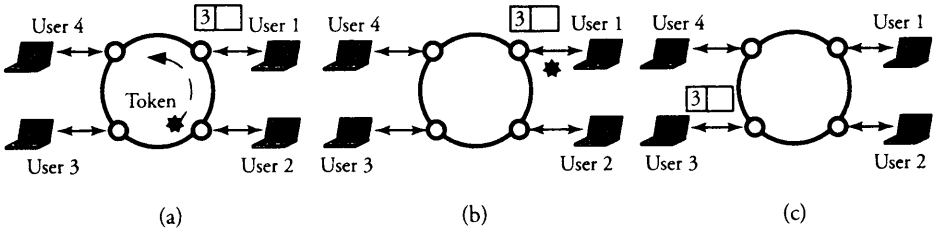


**Figure 5.8** The movement of a frame in a ring-access MAC network

When a user transmits a frame, its repeater forwards the frame to the ring. The frame is circulated completely through the ring. During the circulation of the frame in the ring, each repeater copies the destination address of the frame and examines it. At each stop, if a repeater is the destination, it copies the entire frame. The data is removed by the sender after a complete circulation in the ring. The transmitting user also releases the token to the ring when the following two conditions are met: (1) the transmitting user has finished transmitting the frame and (2) the leading edge of the frame has finished one circulation through the ring and has reached the transmitting user. The advantages of this approach are

- Elimination of the need for acknowledgment
- Convenience of multicasting frames

A repeater plays an important role in the operation of the ring. The repeater goes to the *listen* state when passing the data through the ring and then goes to the *transmit* state when transmitting and receiving data. The repeater can also be in the *bypass* state when its associated user is down or offline. To provide fairness in the system, an upper limit is set on the amount of data each user can transmit at a time. The control mechanism for this scheme can be either centralized or decentralized.

The token-ring scheme is simple, promotes fairness, and provides priority and guaranteed bandwidth. The major flaw with this scheme is maintenance of the token. If the token is lost, the operation of the entire ring is halted. On the other hand, the duplication of token results in frame collisions. For successful ring operations, one user is selected as a monitor to replace a lost token and to ensure that only one token is circulated in the ring.

**Example.** Assume that user 1 in Figure 5.8 needs to transmit a frame to user 3. First, user 1 captures the token and transmits the frame, which circulates through the ring. Since the destination is user 3, user 4 examines the frame and then passes it to the next

user. When the frame reaches user 3, user 3 copies the frame. The frame continues the circulation through the ring until user 1 removes the frame and releases a new token.

**Example.** Now assume that user 1 in Figure 5.8 wants to multicast a frame to users 2 and 3. In this case, user 1 waits until it captures the token and then starts transmission. user 3 copies the frame followed by user 2. Once the frame reaches user 1, it releases the token to the ring and removes the frame from the ring.

### 5.6.2 Token-Ring: IEEE 802.5 Standard

The IEEE 802.5 standard defines the token-ring topology. IEEE 802.5 has also introduced the dedicated token ring, which makes use of a star topology. Users are directly connected to a central hub (concentrator) through full-duplex point-to-point links. This scheme eliminates the use of tokens.

## 5.7 Network of LANs

Increasing the number of interconnected devices and the volume of traffic requires splitting a single large LAN into multiple smaller LANs. Doing so dramatically improves network performance and security but also introduces a new challenge: how to interconnect multiple LANs. LANs may be of different types or may have devices that are not compatible with one another. New protocols need to be developed that allow all partitions of a LAN to communicate with one another.

Multiple LANs can be connected to form a college campus network. The campus backbone serves as a channel between a department and the rest of the campus network and facilitates the connection of the department to the Internet via a gateway router. The campus backbone is an interconnection of routers and switches. Servers used by an entire organization are usually located in a data bank and organization dispatching center.

Devices known as *protocol converters* are used to interconnect multiple LANs. Depending on the level of interconnection required, layer 1, layer 2, layer 3, and layer 4 protocol converters are available. Two networks can be connected using layer 1 devices referred to as *hubs* and *repeaters*. Layer 2 protocol converters have information about the layer 2 protocols on both interconnected LANs and can translate one to the other. At layer 2, *bridges* and *switches* can carry out the task as layer 2 devices. At layers 3 and 4, *routers* and *gateways*, respectively, are used.

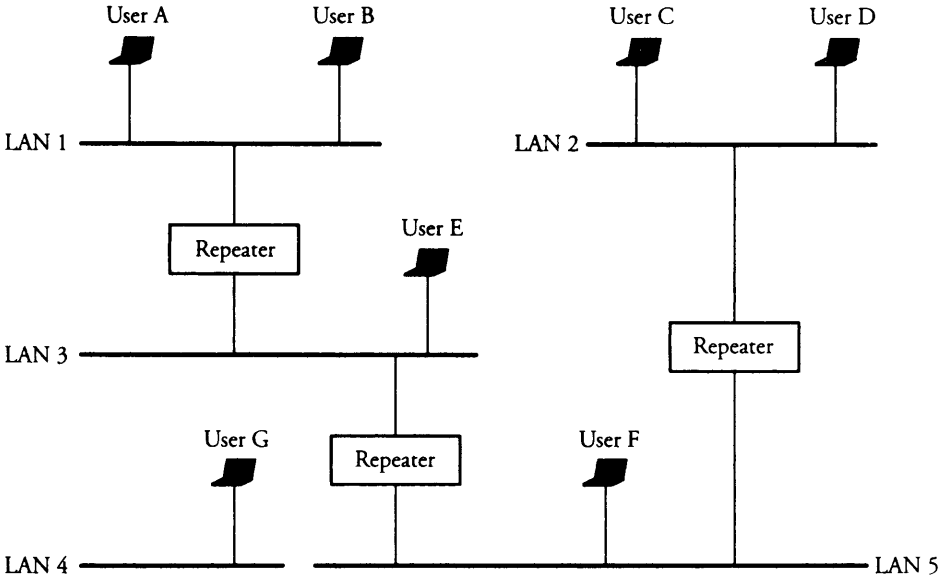


**Figure 5.9** Seven layer 1 users connected through repeaters

## 5.7.1 Using Repeaters, Hubs, and Bridges

In Chapter 3, we explained the operations of repeaters, hubs, and bridges. Figure 5.9 shows a situation in which bus LANs are interconnected through repeaters. Users A–G are connected to multiple Ethernet LANs. Users of these networks are aware of the existence of repeaters and function as a single large LAN. Any user reads all flowing frames sent by other users but accepts those frames that are specifically addressed to it. Thus, collisions may be possible throughout the network if two or more users try to transmit at the same time.

Figure 5.10 depicts a network connection using hubs. A hub is similar to a repeater but copies frames and forwards them to all connected users. As in the case of a repeater, collisions may occur if two or more users try to transmit at the same time. Hubs and repeaters have the following limitations.

- Hubs forward frames to all users. This method of networking results in reduced LAN performance, owing to excess traffic.
- A large number of users are included in the collision domain.
- Security cannot be implemented, since a frame is forwarded to all users.

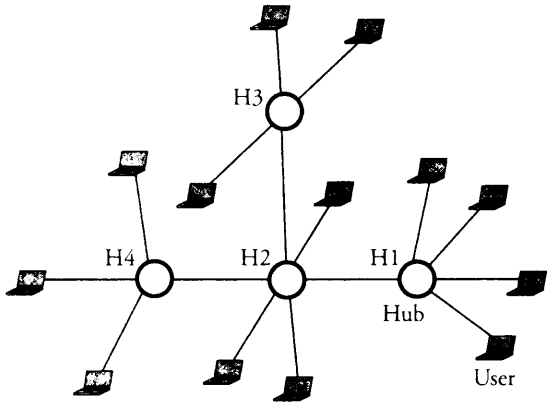


**Figure 5.10** Using hubs in layer 1

### Bridges

Clearly, using a bridge for networking Ethernet LANs can reduce the possibility of collision, as bridges split a LAN system into different collision domains. Because they can selectively retransmit the frame, bridges also offer a greater level of security than repeaters can. Bridges also facilitate communication across multiple LANs and bridges. Sometimes, a bridge that connects two LANs with nonidentical bit rates must have a buffer. A buffer in a bridge holds frames that arrive from a faster LAN directed to a slower LAN. This introduces transmission delay and has adverse effects on the network, causing the flow-control protocols to time out.

Figure 5.11 shows multiple bus LANs being connected by bridges. Suppose that user 1 wants to transmit a frame to user 5. First, bridge B1 examines the destination address and determines whether the forwarded frame is to be delivered to any of the users on LAN 2. If user 3 is not the destination within its connected LANs, the frame can be either dropped or forwarded on LAN2. Making such decisions is a bridge routing capability and depends on how well the routing table of the bridge is structured. Thus, the bridge decides whether to accept or reject a frame at any time.

If it decides to forward a frame on LAN 2, bridge B1 also performs error detection to ensure that the frame is not corrupted. Next, the bridge checks whether LAN 2 and LAN 5 have the same frame format. If they do, the bridge forwards the frame as is. If the frame format is different, it is reformatted to match the frame format of LAN 5. Since a bridge in such scenarios is generally connected to an Ethernet LAN, the bridge has to conform to CSMA/CD while transmitting the frame. When the frame reaches

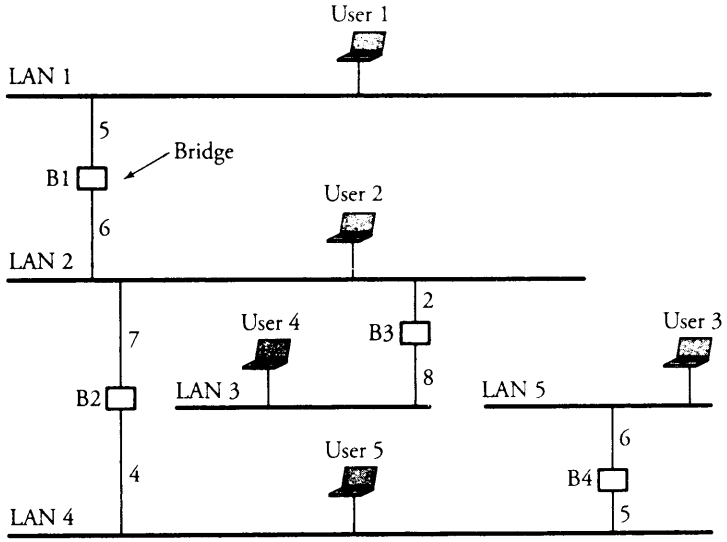


**Figure 5.11** Connecting LANs through bridges

bridges B2 and B3, the same procedure as the one completed in B1 takes place. As a result, B3 rejects the frame, and B2 accepts the frame. The frame is now forwarded on LAN 2. The frame ultimately reaches the destination at user 3 after passing safely over LAN 2, B3, and LAN 3.

A bridge that connects two LANs, such as an Ethernet LAN and a token-ring LAN, has to reformat frames before any transmission. A frame arriving from a token-ring LAN is reformatted to match the Ethernet LAN. As the Ethernet frame format does not contain the priority field, the priority information specified by the token-ring frame is lost. In contrast, a frame arriving from an Ethernet network is assigned a default priority before transmission to the token-ring LAN. Figure 5.12 shows an example in which a LAN using bridges and hubs interconnects a token-ring LAN with several other LANs.

A bridge does not have a global view of its outside network but rather has knowledge only of immediate neighbors. Bridge routing is a process of deciding where to forward received frames. Bridges have this information stored in a table called the *routing table*. Each bridge has multiple subrouting tables for corresponding to all its existing surrounding connected LANs. The routing table consists of the destination address and the destination LAN.

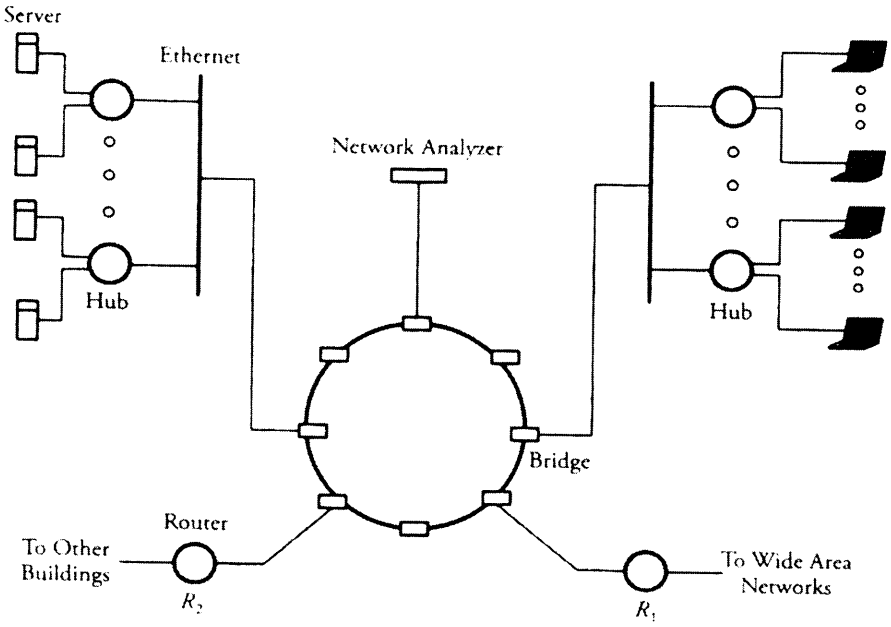


**Figure 5.12** Using bridges and hubs

**Example.** Table 5.1 provides a bridge routing table for B1 and B2 in Figure 5.11. Table 5.2 gives more detail of a routing table for bridge B1. B1 has one routing table for LAN 1 and another routing table for LAN 2. For example, if a frame arrives on LAN 1, the bridge parses the frame for the destination address and looks up the routing table for source LAN 1. If the destination is user 1, the LAN does not need to forward the frame. However, for destinations at user 2, user 3, and user 5, the bridge forwards the frame to LAN 2. For the destination at user 5, the bridge forwards the frame to LAN 4. LAN 1 has five users, LAN 2 has four computers, and LAN 3 has LAN 2 users. Port 1 of the bridge connects to LAN 1, Port 2 of the bridge connects to LAN 2, and port 3 of the bridge connects to LAN 3.

In a static network, connections are fixed, so the routing table entries can be programmed into the bridge: *fixed routing*. In case of any changes to the network, the table entries need to be reprogrammed. This solution is not scalable for large, dynamic networks having frequent user addition and removal. Hence, such networks use an *automatic update* of the routing tables.

**Table 5.1** Routing table for two bridges (B1 and B2) of Figure 5.11

| Dest. from LAN 1 | Next LAN from LAN 1 | Dest. from LAN 2 | Next LAN from LAN 2 | Dest. from LAN 2 | Next LAN from LAN 2 | Dest. from LAN 4 | Next LAN from LAN 4 |
|---|---|---|---|---|---|---|---|
| User 1 | — | User 1 | LAN 1 | User 1 | — | User 1 | LAN 2 |
| User 2 | LAN 2 | User 2 | — | User 2 | — | User 2 | LAN 2 |
| User 3 | LAN 2 | User 3 | — | User 3 | LAN 4 | User 3 | — |
| User 4 | LAN 2 | User 4 | — | User 4 | — | User 4 | LAN 2 |
| User 5 | L2 | User 5 | — | User 5 | LAN 4 | User 5 | — |

Table 5.2 Bridge routing table for bridge B2 in Figure 5.11

| Destination MAC Address | Next LAN |
|---|---|
| 00-40-33-25-85-BB | LAN 1 |
| 00-40-33-25-85-BC | LAN 2 |
| 00-61-97-44-45-5B | LAN 2 |
| 00-C0-96-25-45-C7 | LAN 2 |

In Figure 5.13, for example, if user 1 on LAN 1 sends a frame to user 5 on LAN 1, any corresponding bridge, such as B1 or B5 can figure out that both user 1 and user 5 belong to LAN 1 and forward the frame within LAN 1. Bridge B1 or B2 has the MAC addresses of both user 1 and user 5. Similarly, if user 10 is transmitting a frame to user 11, bridge B5 records the MAC addresses of users 10 and 11 and LAN 3 in its routing table. Each bridge must parse the destination address of an incoming frame in its routing table to determine the association between the destination MAC address and the MAC addresses of the devices connected to its LAN. The bridge scans the routing table to determine whether an association exists and forwards the frame if an entry is in the routing table.

Bridges that update their routing tables are called *transparent bridges* and are typically equipped with the IEEE 802.1d standard. These bridges act as plug-and-play devices and have the capability to build their own routing tables instantaneously. A transparent bridge also has the intelligence to learn about any change in the topology

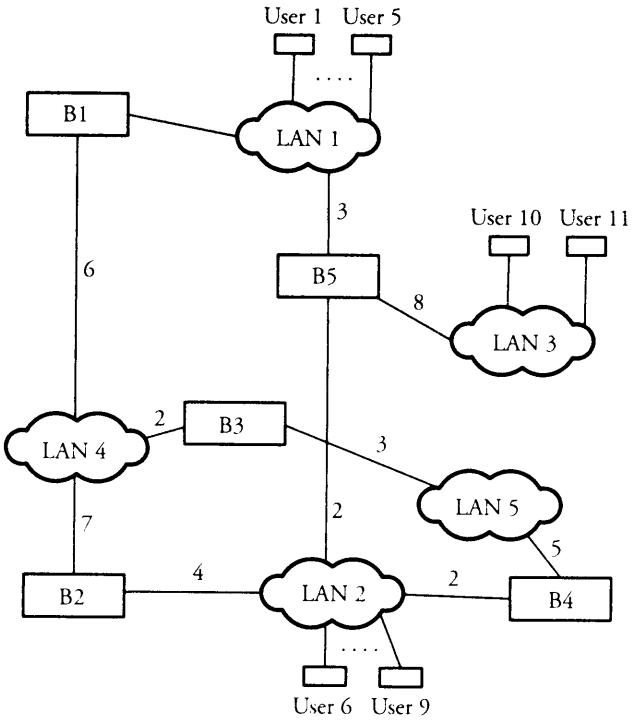


**Figure 5.13** Bridging in local area networks

and to update its routing table. This type of bridge can dynamically build the routing table, based on the information from arriving frames. By parsing the source address of a received frame, a bridge can determine how it can access the local area network of the arriving frame. Based on this information, the bridge updates its routing table.

**Example.** Suppose that frames from user 1 move from LAN 1 to LAN 2 in Figure 5.11. If user 1 transmits a frame to user 2 located in LAN 2, bridge B4 examines its routing table and discovers that the direction on which it received the frame from user 1 is not the same as what it has in its routing table. Hence, bridge B4 updates its routing table.

A bridge initializes its routing tables by using the flooding algorithm. When none of the users in the network have routing table entries, a frame is flooded across the network to all users. If a frame arrives on a bridge that does not have the routing table

entry for the destination, the frame is flooded across all users. As more and more frames are flooded through the network, all bridges will eventually have routing table entries.

**Example.** Interconnection of multiple LANs via bridges can potentially result in the frames circulating indefinitely. One such situation is illustrated in Figure 5.13, where multiple routes are possible between user 1 and user 9. User 1 can reach user 9 via route LAN 1-B1-LAN 4-B2-LAN 2. user 1 can also reach user 9 via LAN 1-B5-LAN 2. With flooding algorithm, a frame released from user 1 being transmitted to user 9 via route LAN 1-B1-LAN 4-B2-LAN 2 can be transmitted back to user 1 via bridge B5, resulting in an infinite loop and hence network congestion.

### Spanning-Tree Algorithm

The *spanning-tree algorithm* is used to overcome the problem of infinite loops in networks with bridges. A spanning tree generates a subset of bridges to be used in the network to avoid loops. The algorithm is as follows

**Begin Spanning-Tree Algorithm**

1. Each link from a bridge to a LAN is assigned a cost. This link cost is inversely proportional to the link's bit rate. A higher bit rate implies a lower cost.
2. Any bridge with the lowest ID is selected as root. A spanning tree is constructed originating from the root bridge. To build the spanning tree, all bridges send a special frame, called a *bridge protocol data unit* (BPDU), comprising a bridge ID and the aggregate cost, from a sender to a receiving user.
3. A receiving bridge compares the sender's bridge ID with its own ID. If the sender's bridge ID is lower, the BPDU is not forwarded. If the sender's bridge ID is higher, the BPDU is stored and forwarded to other users after incrementing the cost. Thus, the bridge determines that it is not the root bridge and stops sending BPDU advertising for the lowest bridge ID. Over a period of time, all bridges, excluding the bridge with the lowest ID, stop sending BPDUs. When the bridge receives no other BPDUs, it declares itself the root bridge.
4. Based on the comparison of all the stored BPDUs, each of the involving bridges determines e least-cost path to the root bridge with an identified port number. This port is called the root port, and any bridge communicates with the root bridge through the root port.
5. Every LAN determines a designated bridge through which it forwards frames. To determine the designated bridge, each bridge sends BPDUs to all LANs to which it is connected. Bridges connected to a particular LAN compare the respective costs to reach the root bridge. The bridge with the lowest cost is designated the root bridge. In case of a tie, the lowest bridge ID determines the designated bridge. ■

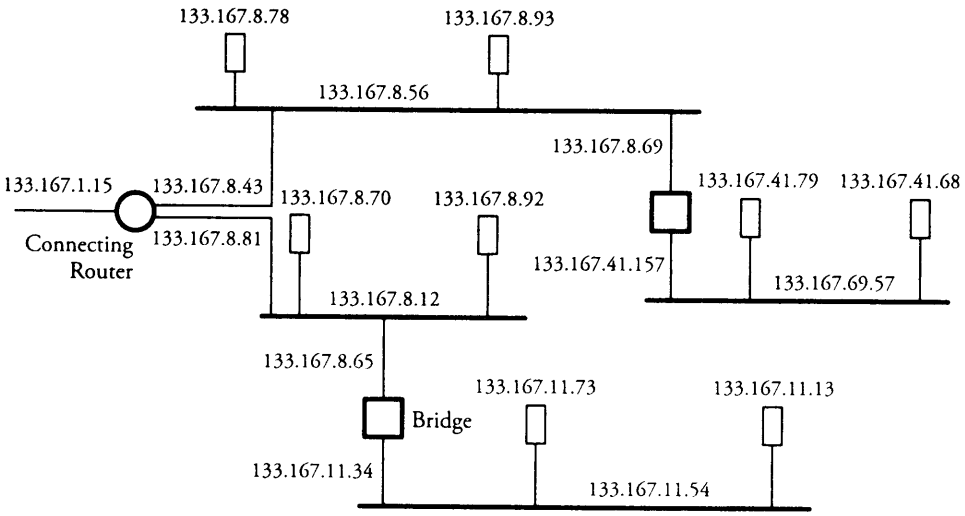


**Figure 5.14** A LAN system and the assignment of IP addresses

**Example.** Figure 5.14 shows that every component of a LAN system is assigned an IP address. Every piece of a LAN cable, including the ones that connect a bridge to a bus, takes an IP address.

## 5.7.2 Layers 2 and 3 Switches

As the complexity of the network system grows, layer 2 devices are not adequate to meet the needs of networks. Users on LANs connected by layer 2 switches have a common MAC broadcast address. Hence, a frame with a broadcast MAC address is forwarded to all users on the network. In a large network, this is considered a large overhead and may result in network congestion. Another issue with layer 2 switches is that to avoid closed loops, there can be only one path between two users. This poses a significant limitation on the performance of large networks. The limitations are overcome by splitting the network into subnets.

Routers, known as layer 3 switches, implement the switching and forwarding functions at the network layer of the protocol stack. The routers are capable of handling heavy traffic loads. Routers are also used to connect multiple subnets in LANs. Routers are sophisticated devices that permit access to multiple paths among users. A router uses software to forward packets or frames. However, the use of software significantly reduces the speed of forwarding frames. But high-speed LANs and high-performance

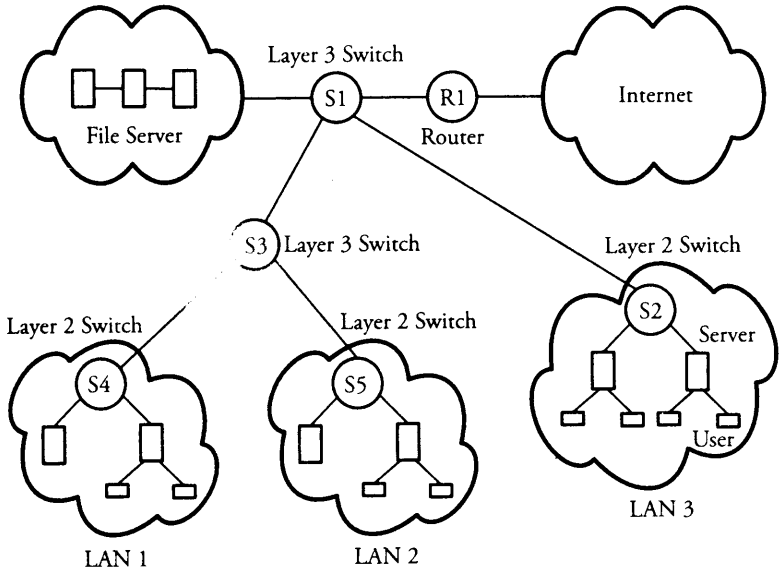


**Figure 5.15** A network with layers 2 and 3 switches

layer 2 switches can operate on millions of frames per second, which mandates layer 3 devices to match the load.

Figure 5.15 shows a typical network scenario in a large organization. The network is split up into subnets, each having a number of desktop systems connected to a layer 2 switch. A layer 3 switch acts as the backbone and connects layer 2 switches through higher-speed links. Servers are connected to either the layer 2 or the layer 3 switch. A software-based router provides the WAN connection.

## 5.8 Summary

A local area network is a communication network that interconnects a variety of data communications devices to serve within a small community. The primary feature of a LAN is its ability to share data and software to provide common services, such as file serving, print serving, support for electronic mail, and process control and monitoring in office and industrial environments. We explored the three basic topologies of LANs—bus, ring, and star—using fundamental knowledge on devices (Chapter 3) and on links (Chapter 4). The simplicity of bus LANs is an advantage when a cable can connect users through its taps. The star topology is a variation on the bus topology,

whereby a hub provides connection capability. Star topology has the advantage of easier installation than bus topology.

For a user to place data onto a local area network, the network must be equipped with a MAC protocol to find ways of sharing its medium. The *Address Resolution Protocol* (ARP) is designed to convert a IP address to a MAC address or vice versa. Two well-known MAC methods are *contention access*, such as CSMA/CD for bus and star topologies, and *round-robin access*, such as token passing or token ring. CSMA/CD operates on a first-come first-served basis and clearly is one of the most popular access protocols. However, its frame collision during high-usage periods is indeed a bottleneck. Round-robin access is more appropriate than CSMA, as the round-robin method can regulate traffic under heavy loads.

We also covered important topics of *internetworking* and the use of repeaters, hubs, and bridges with *switched* LANs. A bridge operates at layer 2 and typically separates users into two collision domains. Routers, known as layer 3 switches, are also used to connect multiple subnets in larger LANs. Routers are typically designed to handle heavy traffic loads.

In Chapter 6, we explore wireless networks. We consider them from two angles: cellular structures and local area networks.

## 5.9 Exercises

1. Consider the transfer of a file containing 1 million characters from one computer to another. Transfer consists of a sequence of cycles. For one cycle, $a$ = (time for data packet + propagation) + (time for ack packet + propagation). The throughput refers to the number of sequences required to transfer 1 million characters. Each character in its digital form requires 8 bits. The two computers are $D = 1$ km apart, and each generates a data rate of $b = 1$ Mb/s, with a packet size $s = 256$ bits, which includes 80 bits of overhead. The propagation speed on the bus is 200 m/$\mu$sec. Find the total elapsed time using throughput and $C$ for the following two cases.
   (a) A bus topology, with each frame acknowledged with an 88-bit frame before the next frame is sent.
   (b) A ring topology having a total circular length of $2D$, with the two computers $D$ distance apart. Acknowledgment is achieved by allowing a frame to circulate past the destination user back to the source user. The ring has $N = 100$ repeaters, each of which introduces a delay of 1 bit time.

2. We want to design a coaxial LAN for 12 offices arranged on three similar floors, each floor having two rows with 2 offices and the rows separated by a hallway. Each office is 5 m × 5 m with a height of 3 m. The LAN center is in the center of the ground floor beneath the three office floors. Assume that each office requires two IP telephone lines and retrieves two Web pages per minute at the average rate of 22 KB per page.
   (a) Estimate the distance from each office to the LAN center.
   (b) Estimate the required available bit rate for the LAN.

3. Consider a 100 m bus LAN with a number of equally spaced computers with a data rate of 100 Mb/s.
   (a) Assume a propagation speed of 200 m/$\mu$s. What is the mean time to send a frame of 1,000 bits to another computer, measured from the beginning of transmission to the end of reception?
   (b) Assume a mean distance between pairs of computers to be 0.375 km, an approximation based on the following observation: For a computer on one end, the average distance is 0.5 km. For a computer in the center, the average distance is 0.25 km. With this assumption, the time to send is transmission time plus propagation time.
   (c) If two computers with a mean distance of 0.37 km start transmitting at the same time, their frames interfere with each other. If each transmitting computer monitors the bus during transmission, how long does it take before it notices a collision? Show your answer in terms of both time and bit time.

4. Consider a 100 Mb/s 100BaseT Ethernet LAN with four attached users, as shown in Figure 5.5. In a nonpersistent CSMA/CD algorithm, a user normally waits $512g$ bit times after a collision before sending its frame, where $g$ is drawn randomly. Assume that a 96 bit times of waiting period are needed for clearing the link from the jammed signal in the 100BaseT Ethernet LAN. Assume that only user 1 and user 4 are active and that the propagation delay between them is 180 bit times. Suppose that these two users try to send frames to each other and that their frames collide at the half-way LAN link. User 1 then chooses $g$ = 2, whereas user 4 picks $g$ = 1, and both retransmit.
   (a) How long does it take for user 1 to start its retransmission?
   (b) How long does it take for user 4 to start its retransmission?
   (c) How long does it take the frame from user 4 take to reach user 1?

5. For a CSMA/CD system, consider the throughput derived from Equation (5.15). Set two parameters in this equation: $\alpha = t_p/T$ and $\beta = \lambda T$.
   (a) Rewrite the throughput in terms of $\alpha$ and $\beta$, and denote it by $U_n$.
   (b) Comment why $R_n$ is in terms of frames/time slot and why $\beta$ can be called "offered load" in this case.
   (c) Using a computer, sketch four plots all in one chart for $U_n$ in terms of $\beta$, given $\alpha = \{0.001, 0.01, 0.1, 1.0\}$, and comment on the behavior of the normalized throughput, $U_n$.
6. For a local area network using CSMA/CD, assume a 12 percent frame error rate owing to noise and errors resulting from collisions. Discuss how the throughput $U$ could be affected.
7. A 10 Gb/s Ethernet LAN with ten users attached to it uses CSMA/CD. The bus is about 10 meters, and users' frames are restricted to a maximum size 1,500 bytes. Based on the statistics, four users in average are active at the same time.
   (a) Find the frame propagation and transmission times.
   (b) Find the average utilization of the bus.
   (c) Find the probability that a user attempts to transmit frames in an empty time slot.
   (d) Find the probability that a user attempts seven different times in seven different empty slots to transmit its frame and is not successful, owing to collision, but is successful on the eighth attempt.
   (e) Find the average number of contentions.
8. Using the CSMA details discussed in this chapter, sketch a block diagram that represents the implementation of this algorithm for the following cases:
   (a) Nonpersistent CSMA
   (b) $p$-persistent CSMA
9. Design (show only the network) a LAN system for a small five-story building. One floor is dedicated to two mail servers and separated three database servers. Each of remaining floor has four computers with broadband access. Your design should meet the following restrictions and conditions: three-input hubs, one bridge, and unlimited Ethernet buses. The incoming broadband Internet access must be connected to a six-repeater ring, no bus LAN is allowed outside of a floor, and a traffic analyzer must be attached to the network.

CHAPTER 6

# Wireless Networks and Mobile IP

In Chapter 4, we reviewed the fundamentals of wireless communication media at the link layer. In this chapter, we explore the concept of wireless networks. Wireless networks are designed for all home and business networking applications and are used in both LANs and WANs. The major topics of the chapter are

- *Infrastructure of wireless networks*
- *Wireless LANs*
- *Protocol layers of wireless LANs*
- *Cellular networks*
- *Mobile IP*
- *Wireless mesh networks (WMNs)*

We start with an overview of wireless communication systems at all levels, from satellite to LANs. We review the protocols and topologies of LANs in the wireless environment, as well as the mobility issue in wireless networks. We then focus on cellular networks, one of the main backbones of our wireless networking infrastructure. At the end of the chapter, we introduce *mobile* IP and *wireless mesh networks*, including WiFi and WiMAX technologies.

## 6.1 Infrastructure of Wireless Networks

Figure 6.1 shows wireless communication systems at all levels. Satellite systems can provide a widespread global coverage for voice, data, and video applications. A satellite orbits the earth while interfacing between a receiver/transmitter pair. The interfacing facilitates the transmission of data to long-distance destinations. Satellite systems are classified according to the orbit distance from the earth:

- *Low-earth orbit*. These satellites orbit the earth at distances between 500 km and 2,000 km and can provide global roaming.
- *Medium-earth orbit*. These satellites orbit the earth at distances of about 10,000 km.

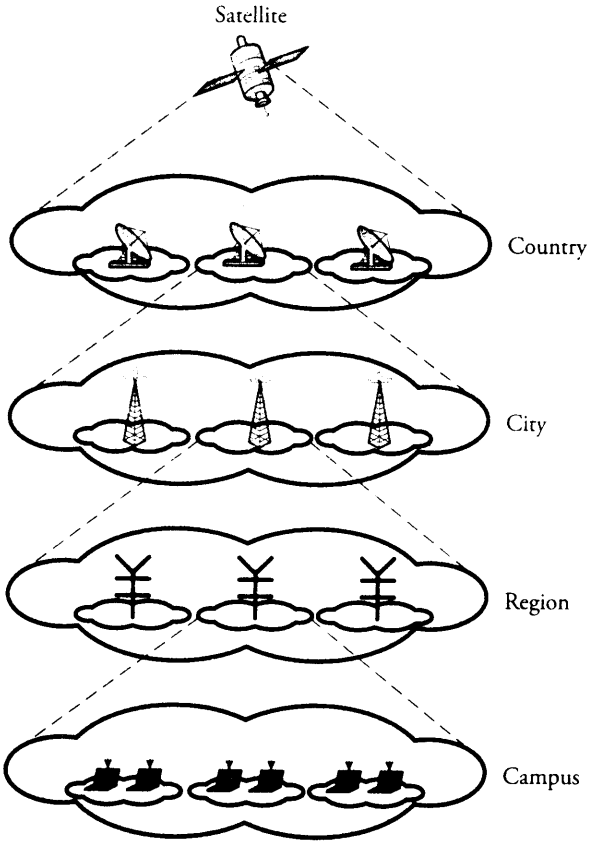


**Figure 6.1** Wireless communication systems, from satellite to LAN

- *Geosynchronous orbit*. These satellites orbit the earth at distances of about 35,800 km. They have a large coverage area and can handle large amounts of data.

Similar to wired networks, wireless networks are hierarchical. However, wireless networks are characterized by limited resources from the perspective of frequency range and available bandwidth. The available bandwidth often varies with time. Wireless networks must be able to adapt to the changing network topology. Wireless network topologies are classified into three main groups:

- Hierarchical
- Star
- Peer to peer (P2P)

The hierarchical architecture acts as a spanning tree and normally covers a large geographical area. The lowest layer of the hierarchy normally represents indoor systems that cover very small areas. The next layer in the hierarchy consists of cellular systems. This hierarchy can be extended to global coverage. The hierarchical topology is ideally suited for large networks. In a star topology, as explained in Chapter 5, nodes are connected to a central hub. Thus, the entire traffic from nodes flows through this central hub. Star networks are used in cellular and paging systems.

Peer-to-peer networks are characterized by pairs of nodes and are normally used in military applications. In these networks, nodes are self-configuring, and various tasks are evenly distributed among nodes. Peer-to-peer networks are multihop networks; a node may use multiple hops to communicate with another node. These networks normally have multiple paths between each two nodes to route around link failures.

## 6.2 Wireless LAN Technologies

Wireless technology helps wired data networks join wireless components. Local area networks can be constructed in wireless fashion mainly so that wireless users moving within a certain organization, such as a university campus, can access a backbone network.

The basic topology in wireless LANs is shown in Figure 6.2 (a). Each user in the wireless network communicates directly with all others, without a backbone network. An improvement to this scheme involves the use of *access points*, or transceivers that can also serve as an interface between the wired and the wireless LANs. Figure 6.2 (b) shows a typical setup with an access point called *wireless switch/hub*. In this scheme, all wireless users transmit to an access point to communicate with users on the wired or

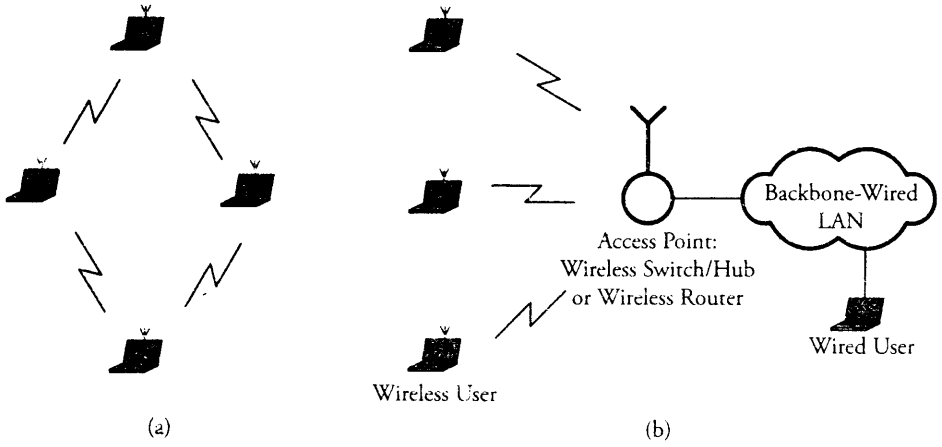


**Figure 6.2** Basic wireless LANs: (a) basic topology; (b) typical setup with access point

wireless LAN. The range of user mobility in a wireless LAN can be extended by using several access points. A mobile user searches for a new access point when the signal level from a nearby access point increases beyond that of its current one. Wireless LAN technologies can be classified into four types: *infrared*, *spread-spectrum*, *narrowband* RF, and *home RF* and *Bluetooth*.

## 6.2.1 Infrared LANs

Each signal-covering cell in an *infrared LAN* is limited to one room. The coverage is small, since the infrared rays cannot penetrate through walls and other opaque obstacles. Infrared communication technology is used in several home devices, such as television remote controls. Three alternative transmission techniques are used for infrared data transmission: *directed beam*, *omnidirectional configuration*, and *diffused configuration*.

The *directed beam* involves point-to-point connections. The range of communications is limited by the transmitted power and the direction of focus. With proper focusing, ranges up to a kilometer can be achieved. This technology can be used in token-ring LANs and interconnections between buildings. The *omnidirectional configuration* consists of a single base station that is normally used on ceilings. The base station sends an omnidirectional signal, which can be picked up by all transceivers. The transceivers in turn use a directional beam focused directly at the base-station unit. In the *diffused-configuration* method, the infrared transmitters direct the transmitted signal

to a diffused reflecting ceiling. The signal is reflected in all directions from this ceiling. The receivers can then pick up the transmitted signal.

The use of infrared has several advantages. For example, the bandwidth for infrared communication is large and can therefore achieve high data rates. Also, because infrared rays are reflected by lightly colored objects, it is possible to cover the entire area of the room with reflections from objects. Since infrared cannot penetrate through walls and other opaque obstacles, it becomes very difficult for any adversary to carry out a passive attack or to eavesdrop. Hence, communication with infrared technology is more secure. Also, separate infrared networks can be used in adjacent rooms without any interference effects. Finally, equipment for infrared communication is much cheaper than microwave communication. The one major disadvantage of infrared technology is that background radiation from sunlight and indoor lighting can cause interference at the infrared receivers.

### 6.2.2 Spread-Spectrum LANs

*Spread-spectrum LANs* operate in industrial, scientific, and medical applications, making use of multiple adjacent cells, each having a different center frequency within a single band to avoid any interference. Within each of these cells, a star or peer-to-peer topology can be deployed. If a star topology is used, a hub as the network center is mounted on the ceiling. This hub, serving as an interface between the wired and wireless LANs, can be connected to other wired LANs. All users in the wireless LAN transmit and receive signals from the hub. Thus, the traffic flowing among users moves through the central hub. Each cell can also deploy a peer-to-peer topology. The spread-spectrum techniques use three different frequency bands: 902–928 MHz, 2.4 GHz–2.4835 GHz, and 5.725 GHz–5.825 GHz. Higher-frequency ranges offer greater bandwidth capability. However, the higher-frequency equipment is more expensive.

### 6.2.3 Narrowband RF LANs

*Narrowband radio frequency* (RF) LANs use a very narrow bandwidth. Narrowband RF LANs can be either licensed or unlicensed. In licensed narrowband RF, a licensed authority assigns the radio frequency band. Most geographic areas are limited to a few licenses. Adjacent cells use different frequency bands. The transmissions are encrypted to prevent attacks. The licensed narrowband LANs guarantee communication without any interference. The unlicensed narrowband RF LANs use the unlicensed spectrum and peer-to-peer LAN topology.

### 6.2.4 Home RF and Bluetooth

The *home RF* is a wireless networking standard that operates in the 2 GHz frequency band. Home RF is used to interconnect the various home electronic devices, such as desktops, laptops, and appliances. Home RF supports data rates of about 2 Mb/s and both voice and data and has a range of about 50 meters. *Bluetooth* is a technology to replace the cables necessary for short-range communication within 10 meters, such as between monitors and CPU, printer and personal computers, and so on. Bluetooth technology also eliminates the need for cables in laptops and printers. Bluetooth operates at 2.4 GHz frequency band and supports data rates of 700 Kb/s.

## 6.3 IEEE 802.11 Wireless Standard

Each wireless LAN user in Figure 6.2 (b) has a wireless LAN adapter for communication over the wireless medium. This adapter is responsible for authentication, confidentiality, and data delivery. To send data to a user in the wired LAN, a user in the wireless LAN first sends the data packet to the access point. The access point recognizes the wireless user through a unique ID called the *service-set identification* (SSID). SSID is like a password-protection system that enables any wireless client to join the wireless LAN. Once the wireless user is authenticated, the access point forwards data packets to the desired wired user through the switch or hub.

Access points build a table of association that contains the MAC addresses of all users in the wireless network. The access point uses this information for forwarding data packets in the wireless network. Figure 6.3 shows a setup whereby the LANs in two buildings are interconnected by *wireless bridges*. A wireless bridge is basically the same as a regular bridge but is equipped with a wireless transceiver. The most common medium for wireless networks is radio waves at a frequency of 2.4 GHz band. Wireless bridges are also used to interconnect LANs in different buildings. The access range of wireless LANs can be extended by deploying a greater number of access points.

Figure 6.4 shows multiple access points being used to extend the connectivity range of the wireless network. The area of coverage of each access point can be overlapped to adjacent ones to provide seamless user mobility without interruption. Radio signal levels in a wireless LAN must be maintained at an optimum value. Normally, a site survey must be conducted for these requirements. Site surveys can include both indoor and outdoor sites. The surveys are normally needed for power requirements, placement of access points, RF coverage range, and available bandwidth.

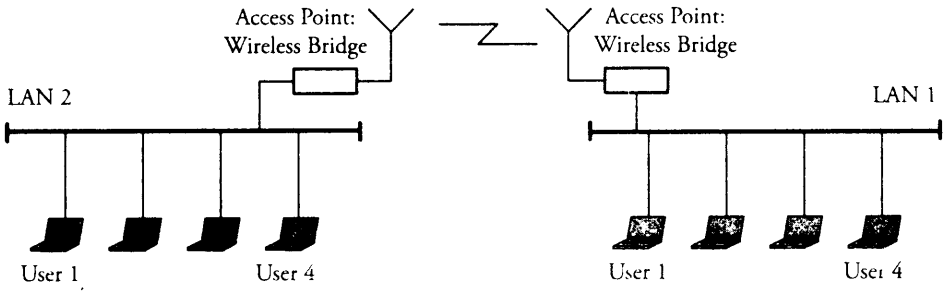


**Figure 6.3** Connecting two LANs through wireless bridges

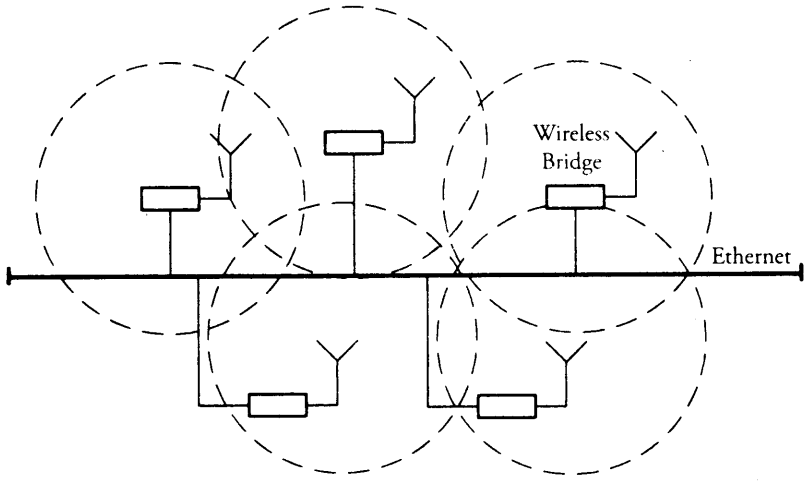


**Figure 6.4** Use of multiple access points to extend the range of wireless access

The transmission media used in high-speed LANs are twisted pair and fiber-optic cables. The use of wireless media presents a few advantages, such as user mobility and reduced cost of transmission media. User mobility enables users to access the network resources from any point in the geographic area. Wireless LANs must be reliable and secure in order to be widely deployed. The standards for wireless LANs include 802.11 and its family: 802.11a, 802.11b, and 802.11g. Standard 802.11 typically uses the *Carrier Sense Multiple Access* with *collision* avoidance (CSMA/CA) method (see Chapter 5). With this method, each user listens for traffic coming from other users and transmits data if the channel is idle. If the channel is busy, the user waits until the channel becomes idle. The user then transmits data after a random *back-off time*. This is done to prevent

all users from transmitting at the same time when the channel becomes idle. The details of the 802.11 standards are explained further in the next two subsections.

The IEEE 802.11 wireless LAN standard defines services for physical, MAC layer, and MAC management protocols. The physical layer is responsible for transmitting raw data over RF or infrared media. The MAC layer resolves access control issues and ensures privacy of transmitted data and reliability of data services. The management protocols ensure authentication and data delivery.

### 6.3.1 802.11 Physical Layer

IEEE 802.11 operates in the 2.4 GHz band and supports data rates of 1 Mb/s to 2 Mb/s. IEEE 802.11a operates in the 5 GHz band and supports data rates of up to 54 Mb/s. IEEE 802.11b operates in the 2.4 GHz band and supports data rates of 5.5 Mb/s to 11 Mb/s. IEEE 802.11g operates at 2.4 GHz and supports even higher data rates.

The IEEE 802.11 physical layer is of four types.

1. *Direct-sequence spread spectrum* (DSSS) uses seven channels, each supporting data rates of 1 Mb/s to 2 Mb/s. The operating frequency range is 2.4 GHz ISM band. DSSS uses three nonoverlapping channels in the 2.4 GHz ISM band. The 2.4 GHz frequency band used by 802.11 results in interference by certain home appliances, such as microwave ovens and cordless telephones, which operate in the same band.
2. *Frequency-hopping spread spectrum* (FHSS) uses a pseudonoise sequence and signal hopping from one channel to another. This technique makes use of 79 channels. FHSS operates in the 2.4 GHz ISM band and supports data rates of 1 Mb/s to 2 Mb/s.
3. *Infrared* with an operating range of about 20 meters operates on a broadcast communication paradigm. A *pulse position modulation* (PPM) scheme is used.
4. *Orthogonal frequency division multiplexing* (OFDM), explained in Chapter 4, is a multicarrier modulation scheme whereby the carrier spacing is carefully selected so that each subcarrier is orthogonal to the other subcarriers. Two signals are *orthogonal* if they are multiplied together and their integral over an interval is 0. Orthogonality can be achieved by letting the carrier spacing be equal to the reciprocal of the useful symbol period. As the subcarriers are orthogonal, the spectrum of each carrier has a null at the center frequency of each of the other carriers in the system. This results in no interference between the carriers, allowing them to be spaced as close as possible.

*IEEE 802.11a* uses OFDM, which uses 12 orthogonal channels in the 5 GHz range. This reduces the interference from other home appliances, unlike the case with 802.11b. The two standards 802.11a and 802.11b can operate next to each other without any interference: 802.11a equipment is more expensive and consumes more power, as it uses OFDM. The frequency channels are nonoverlapping. IEEE 802.11a operates in the 5 GHz band. The achievable Mb/s data rates are 6, 9, 12, 18, 24, 36, 48, and 54. Convolution coding is used for forward error correction.

*IEEE 802.11b* uses DSSS but supports data rates of up to 11 Mb/s. The modulation scheme employed is called *complementary code keying* (CCK). The operating frequency range is 2.4 GHz and hence can interfere with some home appliances. *IEEE 802.11g* achieves very high data rates compared to 802.11b and uses the 2.4 GHz frequency band. A combination of encoding schemes is being used in 802.11g. An 802.11g client can operate with an 802.11b access point; similarly, an 802.11b client can operate with an 802.11g access point.

## 6.3.2 802.11 MAC Layer

IEEE 802.11 provides several key functionalities: reliable data delivery, media access control, and security features. *Reliable data delivery* is a key feature available in the MAC layer of IEEE 802.11. The imperfections of the wireless medium, such as noise, interference, and multipath effects, may lead to frame loss. IEEE 802.11 uses acknowledgment (ACK) to ensure reliable data delivery. When a source sends a data frame, the destination responds with an ACK to acknowledge receipt of the frame. If the source does not receive an ACK for a certain period of time, it times out the process and retransmits the frame.

The *request-to-send/clear-to-send* (RTS/CTS) scheme also is used to further enhance reliability. When it has data to send, a source sends an RTS signal in the form of a frame to the destination. The destination sends a CTS signal if it is ready to receive data. The source sends the data frame after receiving the CTS signal from the destination. The destination then responds with an ACK to indicate successful receipt of data. This four-way handshake leads to a greater reliability of data delivery. When a source sends an RTS frame, users within the reception range of the source avoid sending any frames during this interval, to reduce the risk of collisions. For the same reason, when the destination sends a CTS frame, users in the reception range of the destination refrain from sending any frames during this interval.

Another key functionality is *media access control* (MAC). Media-access algorithms are of two types: *distributed access* and *centralized access*. In distributed-access protocols,

media access control is distributed among all the nodes. Nodes use a carrier-sense mechanism to sense the channel and then transmit. Distributed-access protocols are used in ad hoc networks with highly bursty traffic. In centralized-access protocols, the media-access issues are resolved by a central authority. Central-access protocols are used in some wireless LANs that have a base-station backbone structure and in applications that involve sensitive data. The IEEE 802.11 MAC algorithm provides both distributed- and centralized-access features. Centralized access is built on top of distributed access and is optional.

The MAC layer consists of two sublayers: the *distributed-coordination function* (DCF) algorithm and the *point-coordination function* algorithm (PCF).

### Distributed Coordination Function (DCF) Algorithm

The DCF algorithm uses contention resolution, and its sublayer implements the CSMA scheme for media access control and contention resolution. As explained in Chapter 5, a CSMA sender listens for traffic on the medium. If it senses that the medium is idle, it transmits; otherwise, if the medium is busy, the sender defers transmission until the medium becomes idle. DCF has no provisions for collision detection, which is difficult in wireless networks because of the hidden-node problem. To overcome this problem, the interframe space (IFS) technique is used. IFS is a delay whose length is based on frame priority. IFS has three timing levels. The steps in the algorithm follow.

**Begin DCF Algorithm for Wireless 802.11 MAC**

1. The sender senses the medium for any ongoing traffic.
2. **If** the medium is idle, the sender waits for a time interval equal to IFS. Then the sender senses the medium again. If the medium is still idle, the sender transmits the frame immediately.
   **If** the medium is busy, the sender continues to sense the medium until the medium becomes idle.
3. Once the medium becomes idle, the sender delays its activity by a time interval equal to IFS and senses the medium again.
4. **If** the medium is still idle, the sender backs off for an exponential time interval and senses the medium again after that interval.
   **If** the medium continues to be idle, the sender transmits immediately.
   **If** the medium becomes busy, the sender stops the back-off timing and restarts the process once the medium becomes idle. ■

The IFS time-interval technique is based on the priority of the data. The three timing intervals used for IFS are:

1. *Short IFS* (SIFS). This timing interval is used if immediate response is required. A sender using a SIFS has highest priority. SIFS is used to send ACK frames. A user receiving a frame directed to only itself responds with an ACK after a time interval equal to SIFS. The SIFS time interval compensates for the lack of a collision-detection system in wireless networks.
2. *Point IFS coordination function* (PIFS). This timing interval is used by the central authority or controller in the PCF scheme.
3. *Distributed IFS coordination function* (DIFS). This timing interval is used for the normal asynchronous frames. Senders waiting for the DIFS interval have the least priority.

### Point Coordination Function

The *point-coordination function* (PCF) provides a contention-free service. PCF is an optional feature in IEEE 802.11 and is built on top of the DCF layer to provide centralized media access. PCF includes a *polling feature* implemented at the centralized polling master (point coordinator). The point coordinator uses the PIFS interval to issue polls. Since this interval is greater than the DIFS interval, the coordinator effectively restrains all asynchronous traffic when issuing a poll. The protocol defines an interval called the *superframe interval*, which consists of a contention-free period that the point coordinator used to issue polls. The other interval is the contention period used for stations to send normal asynchronous data. The next superframe interval begins only after the medium becomes idle. The point coordinator has to wait during this period to gain access.

### MAC Frame

The frame format for the 802.11 MAC is shown in Figure 6.5 and is described as follows.

- *The frame control* (FC) field provides information on the type of frame: control frame, data frame, or management frame.
- *Duration/connection* ID (D/I) refers to the time allotted for the successful transmission of the frame.
- *The addresses* field denotes the 6-byte source and destination address fields.

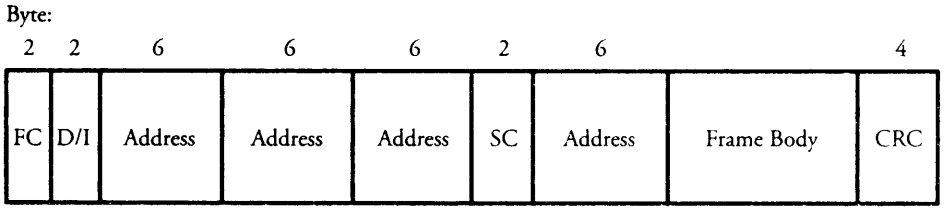


**Figure 6.5** IEEE 802.11 MAC frame

- *The sequence control* (SC) field consists of 4 bits reserved for fragmentation and reassembly and 12 bits for a sequence number of frames between a particular transmitter and receiver.
- *The frame body* field contains a MAC service data unit or control information.
- *The cyclic redundancy check* (CRC) field is used for error detection.

The three frame types in IEEE 802.11 are *control frames*, *data-carrying frames*, and *management frames*. Control frames ensure reliable data delivery. The types of control frames are

- *Power save–poll* (PS–Poll). A sender sends this request frame to the access point. The sender requests from the access point a frame that had been buffered by the access-point because the sender was in power-saving mode.
- *Request to send* (RTS). The sender sends an RTS frame to the destination before the data is sent. This is the first frame sent in the four-way handshake implemented in IEEE 802.11 for reliable data delivery.
- *Clear to send* (CTS). The destination sends a CTS frame to indicate that it is ready to accept data frames.
- ACK *frame*. The destination uses this frame to indicate to the sender a successful frame receipt.
- *Contention-free end* (CFE). The PCF uses this frame to signal the end of the contention-free period.
- CFE/End + CFE/ACK. PCF uses this frame to acknowledge the CFE end frame.

The data-carrying frames are of the following types:

- *Data*. This is the regular data frame and can be used in both the contention and contention-free periods.

- *Data/CFE-ACK*. This is used for carrying data in the contention-free period and is used to acknowledge received data.
- *Data/CFE-Poll*. PFC uses this frame to deliver data to destinations and to request data frames from users.
- *Data/CFE ACK/CFE-Poll*. This frame combines the functionalities of the previous three frames into one frame.

Management frames are used to monitor and manage communication among various users in the IEEE 802.11 LAN through access points.

### 6.3.3 WiFi Technology and 802.11

*Wireless fidelity* (WiFi)—a term trademarked by the WiFi Alliance—technology is a set of standards for wireless local area networks (WLANs). WiFi allows mobile devices, such as laptop computers, digital cameras, and personal digital assistants (PDAs), to connect to local area networks. WiFi is also intended for Internet access and wireless voice over IP (VoIP) phones. Computers can also have built-in WiFi, allowing offices and homes to be networked without expensive wiring.

Figure 6.6 shows three WiFi networks connected to the Internet through *wireless routers with gateway/bridge*. A wireless router with gateway/bridge is a router that can provide radio communications to certain wireless access points, as well as routing to wired Internet devices. Such router/gateways can also communicate with one another. For example, in Figure 6.6, routers A and B are communicating directly to establish

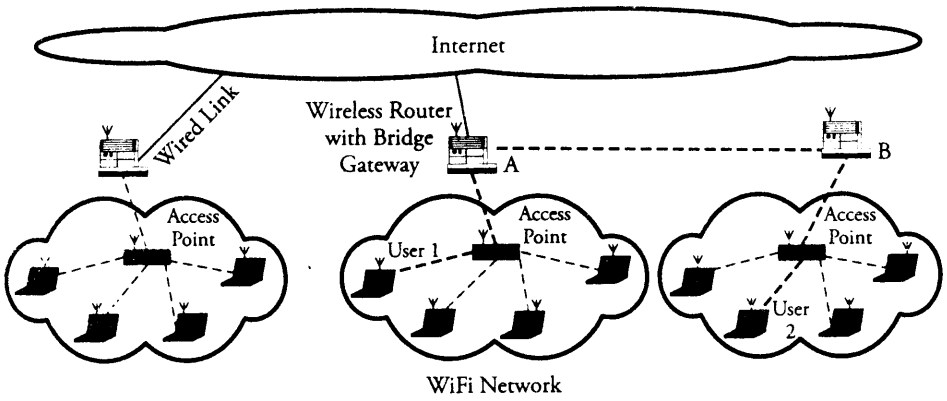


**Figure 6.6** Connectivity of wireless users to WiFi access points to reach the Internet and direct wireless connections

connection for WiFi users 1 and 2; these two users could also be connected through the Internet. However, because an Ethernet uses contention access in WiFi, all users wanting to pass data through an access point contend for its attention on a random basis. This can cause nodes distant from the access point to be interrupted by closer nodes, resulting in reducing their throughput.

The connection is made by radio link signals. A *hotspot* is defined as an access point in a geographical region covered by WiFi. The range of an access point built into a typical WiFi home router is 50 meters indoors and 90 meters outdoors. WiFi is based on the IEEE 802.11 standard. The most widespread version of WiFi is based on IEEE 802.11b/g operating over 11 channels (5 MHz each), centered on Channel 1 at 2,412 MHz all the way to Channel 11 at 2,462 MHz. In the United States, maximum transmitter power is 1 watt, and maximum effective radiated power is 4 watts.

Several routing protocols are used to set up WiFi devices. One of these protocols is the *Optimized Link State Routing* (OLSR) protocol developed for mobile networks. OLSR operates as a table-driven and proactive protocol (see Chapter 19 for details). Thus, it regularly exchanges topology information with other nodes of the network. Nodes are selected as multipoint relays by some neighboring nodes. They exchange this information periodically in their control messages. With WiFi, most networks rely heavily on open source software or even publish their setup under an open source license.

WiFi allows LANs to be deployed without cabling, thereby lowering the cost of network deployment and expansion. WiFi may be used in places where cables cannot be laid. However, the use of the 2.4 GHz WiFi band does not require a license in most of the world, provided that one stays below the local regulatory limits and accepts interference from other sources, including interference that causes devices to no longer function.

However, the 802.11b and 802.11g standards over the 2.4 GHz spectrum used for WiFi are crowded with other equipment, such as Bluetooth devices, microwave ovens, and cordless phones. This may cause degradation in performance, preventing the use of open access points by others. In addition, the power consumption is fairly high compared to that for other standards, making battery life and heat a concern.

## 6.4 Cellular Networks

Cellular networks use a networked array of transceiver *base stations*, each located in a *cell* to cover the networking services in a certain area. Each cell is assigned a small frequency band and is served by a base station. Neighboring cells are assigned different frequencies

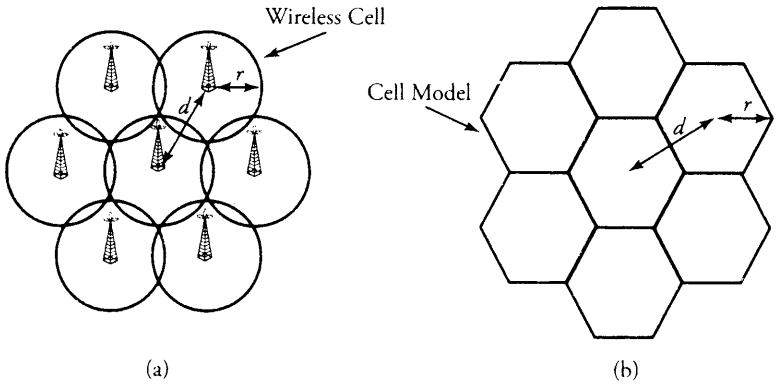


**Figure 6.7** Cellular partitions: (a) real areas; (b) modeled areas

to avoid interference. However, the transmitted power is low, and frequencies can be reused over cells separated by large distances. The hexagonal pattern of a cell is chosen so that the distance $d$ between the centers of any two adjacent cells becomes the same. Distance $d$ is given by

$$d = \sqrt{3}r, \tag{6.1}$$

where $r$ is the cell radius. A typical practical value for the cell radius is 3 km to 5 km. First-generation cellular networks were analog and used FDMA for channel access. Second-generation cellular networks were digital, using CDMA channel-access techniques. With the advent of the third- and later-generation cellular networks, multimedia and voice applications are supported over wireless networks. A covered area of a cellular network is visualized and approximated by a hexagonal cell served by its own antenna at the center of the hexagon, as shown in Figure 6.7.

## 6.4.1 Connectivity

Figure 6.8 shows the connectivity of two mobile users in cellular systems. A cell base station at the center of a cell consists of an *antenna*, a *controller*, and a *transceiver*. The base station is connected to the *mobile switching center* (MSC). An MSC serves several base stations and is responsible for *connecting calls* between mobile units. In Figure 6.8, an MSC is connected to two base stations, A and B. An MSC is also connected to the public telephone system to enable communication between a fixed subscriber and mobile subscriber. An MSC also manages mobility and accounting for user billing.

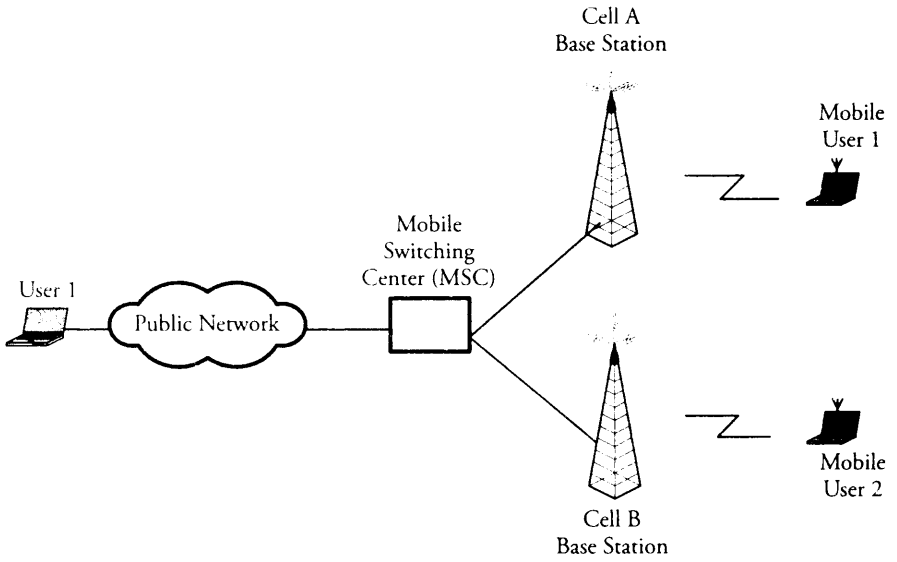


**Figure 6.8** Connectivity of mobile users in cellular systems.

The steps involved in establishing a call between two mobile users in a cellular network are as follows:

1. *Mobile unit setup*. When the mobile unit is switched on, it searches for the strongest control channel. The mobile user is assigned a base station with which it operates. A handshake of messages takes place between the associated MSC and the mobile user through the base station. The MSC registers and authenticates the user through the base station. If the user moves to a new cell, this step repeats in the new cell.
2. *Originated call*. When a mobile originates a call, the called number is sent to the base station, from where it is forwarded to the MSC.
3. *Paging*. MSC pages specific base stations, based on the called number. The base stations in turn send a paging message on their set-up channel to locate the called user, as shown in Figure 6.9.
4. *Call accepting*. When the base station pages all users in its cell, the called user recognizes its number and responds. The base station then notifies the MSC, which sets up a connection between the called and calling base-station units.

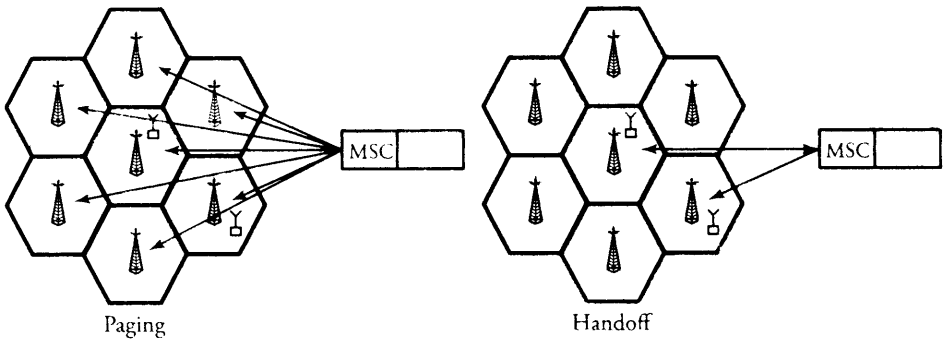


**Figure 6.9** Basic operation of cellular systems

5. *Ongoing call*. Once the connection is established, exchange of data and voice occur between the two communicating mobile units through the base stations and the MSC.
6. *Handoff*. A handoff occurs when a mobile unit moves from one cell to another. The traffic channel switches to the new base station, using the MSC, as shown in Figure 6.9. This switch appears seamless to the user, without any interruption of the traffic.
7. *Call blocking*. When a mobile user originates a call, a busy tone is returned to the user if all the traffic channels to the base station are busy.
8. *Call termination*. When one of the users in a mobile conversation hang up, the MSC is informed of the call termination, and the traffic channels are deallotted at both base stations.
9. *Call drop*. When a base station cannot maintain a minimum signal level during a call, the call is dropped. Weak signals may occur because of interference or channel distortions.

The preceding operations use two types of channels for communication between the mobile and a base station, depending on the application of an operation. These two types of channels are *control channel* and *traffic channel*. Control channels are used for call setup and maintenance. This channel carries control and signaling information. Traffic channels carry the data between the users. Calls between fixed and mobile subscribers are also possible. An MSC can connect to the public telephone system and enable the connection between a mobile user and a fixed subscriber.

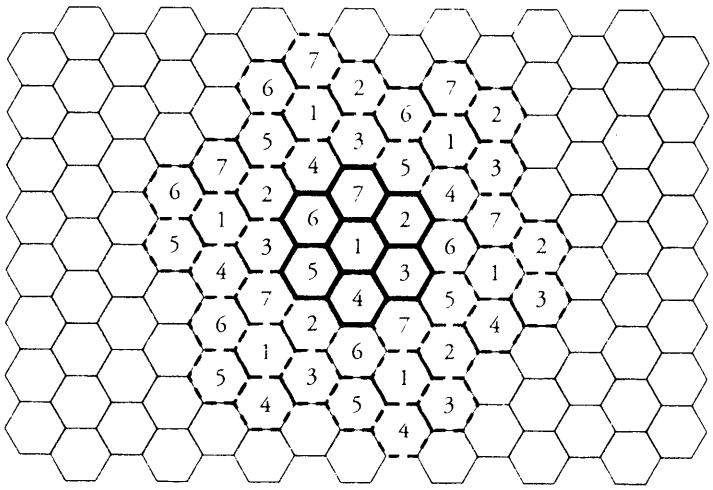

**Figure 6.10** Cell clusters and frequency reuse among seven-cell clusters

## 6.4.2 Frequency Reuse

The basic idea of *frequency reuse* is that if a channel of a certain frequency covers an area, the same frequency can be reused to cover another area. The transmission power of the antenna in a cell is limited to avoid energy from escaping into neighboring cells. We define a *reuse cluster of cells* as $N$ cells in which no frequencies are identical. Two *cochannel cells* are then referred to two cells in which a frequency in one cell is reused in the other one. Figure 6.10 shows a frequency-reuse pattern in a cellular network. In this example, each cluster has seven cells, and those cells with the same numbers are cochannel cells.

Let $F$ be the total number of frequencies allotted to a cluster with $N$ cells. Assuming that all cluster cells share an equal number of frequencies, the number of channels (frequencies) each cell can accommodate is

$$c = \frac{F}{N}. \tag{6.2}$$

A cluster can be replicated many times. If $k$ is the number of times a cell is replicated, the total number of channels in the cellular system—so-called *system capacity*—is derived by

$$C = kF = kcN. \tag{6.3}$$

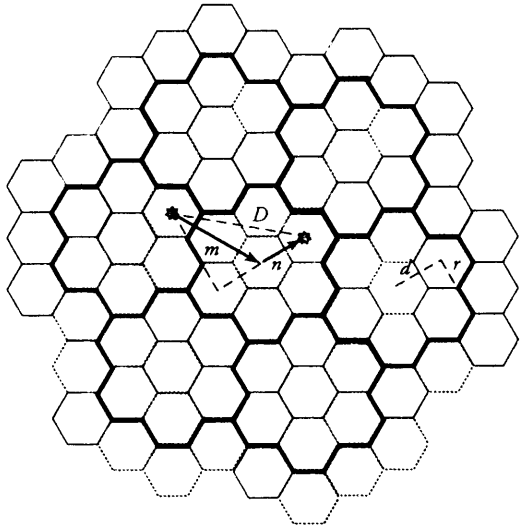


**Figure 6.11** Nearest cochannel cells

In order to determine the location of a cochannel cell, we start from the center of a cell and move $m$ cells or $md$ km to any direction, then turn 60 degrees counterclockwise, and, finally, move $n$ cells or $nd$ km until we reach a cell with the same frequency. As shown in Figure 6.11, we have a case with $m = 3$ and $n = 1$. With a simple geometric manipulation of this situation, we can calculate the distance between the center of the nearest neighboring cochannel cell, $D$, shown in Figure 6.11:

$$\begin{aligned} D &= \sqrt{(nd \cos 30)^2 + (md + nd \sin 30)^2} \\ &= d\sqrt{m^2 + n^2 + mn}. \end{aligned} \tag{6.4}$$

As the distance between the centers of any two adjacent cells is $d = \sqrt{3}r$ according to Equation (6.1), we can rewrite Equation (6.4) as

$$D = r\sqrt{3(m^2 + n^2 + mn)}\,. \tag{6.5}$$

If we connect all the centers of all hexagons for "1" cochannel cells—the same arguments can be made for 2, 3, . . . cochannel cells—we make a larger hexagon, covering $N$ cells with radius $D$. Knowing that the area of a hexagon is approximately

2.598 × (square of its radius), we can derive the ratio of the areas of the $r$-radius hexagon, $A_r$, and $D$-radius hexagon $A_D$ as

$$\frac{A_r}{A_D} = \frac{2.598r^2}{2.598D^2}. \tag{6.6}$$

Combining Equations (6.5) and (6.6), we calculate the area ratio as

$$\frac{A_r}{A_D} = \frac{1}{3(m^2 + n^2 + mn)}. \tag{6.7}$$

From the geometry, we can easily verify that the $D$-radius hexagon can enclose $N$ cells plus 1/3 of the cells from each six overlapping peripheral $D$-radius hexagons. Consequently, the total number of cells covered in a $D$-radius hexagon is $N + 6(1/3)N = 3N$. Then, $\frac{A_r}{A_D} = \frac{1}{3N}$, and Equation (6.7) can be simplified to

$$N = m^2 + n^2 + mn. \tag{6.8}$$

This important result gives an expression for the size of the cluster in terms of $m$ and $n$. As the number of users in a cellular network increases, frequencies allotted to each cell may not be sufficient to properly serve all its users. Several techniques can be used to overcome these problems, as follows:

- *Adding new channels*. As networks grow in size and cells expand, channels can be added to accommodate a large number of users.
- *Frequency borrowing*. When a cell becomes congested, it can borrow frequencies from adjacent cells to handle the increased load.
- *Cell splitting*. In areas with a high volume of usage, cells are split into smaller cells. The power level of the transceiver is reduced to enable frequency reuse. But smaller cells increase the number of handoffs that take place as the user moves from one cell to another more often.
- *Cell sectoring*: A cell can be partitioned into sectors, with each sector containing its own subchannel.
- *Microcells*. In congested areas, such as city streets and highways, microcells can be formed. In a smaller cell, the power levels of the base station and mobile units are low.

**Example.** Consider a cellular network with 64 cells and a cell radius of $r = 2$ km. Let $F$ be 336 traffic radio channels and $N = 7$. Find the area of each cell and the total channel capacity.

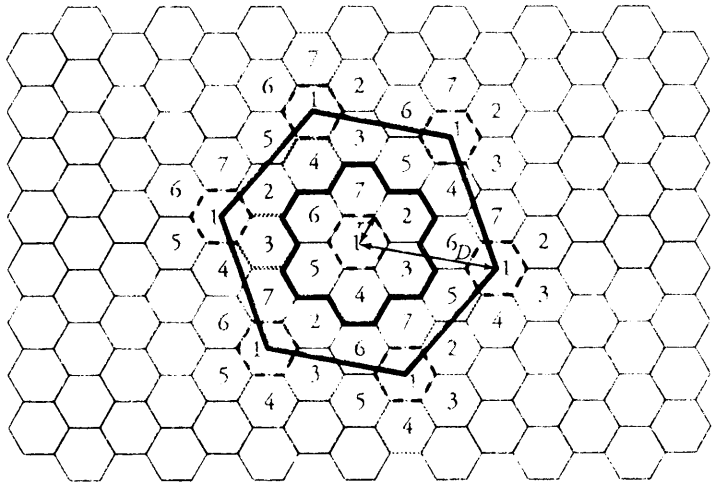

**Figure 6.12** Forming a $D$-radius cluster by connecting all cell 1 centers

***Solution.*** Each hexagon has an area of $1.5\sqrt{3}r^2 = 10.39\ \text{km}^2$. The total area covered by the hexagonal cells is $10.39 \times 64 = 664.69^2$. For $N = 7$, the number of channels per cell is $336/7 = 48$. Therefore, the total channel capacity is equal to $48 \times 64 = 3{,}072$ channels.

## 6.4.3 Local and Regional Handoffs

When it moves to a new cell, a wireless terminal requests a *handoff* for a new channel in the new cell. The increase in traffic volume and demand, as well as seamless, high-performance handoff in wireless systems are expected. A successful handoff operation requires certain criteria to be achieved. When a wireless terminal moves from one base-station cell to another, handoff protocols reroute the existing active connections in the new cell. The challenges in wireless networks are to minimize the packet loss and to provide efficient use of network resources while maintaining quality-of-service (QoS) guarantees. Robustness and stability must also be taken into consideration for handoff protocol design. Robustness and stability are especially important when interference or fading in the radio channel results in a request-handoff operation by a wireless terminal.

Cellular networks typically have three types of handoffs, as shown in Figure 6.13: *channel*, *cell*, and *regional*. *Channel handoff* involves transferring a call between channels in a cell. The wireless terminal first initializes a request for a channel change to

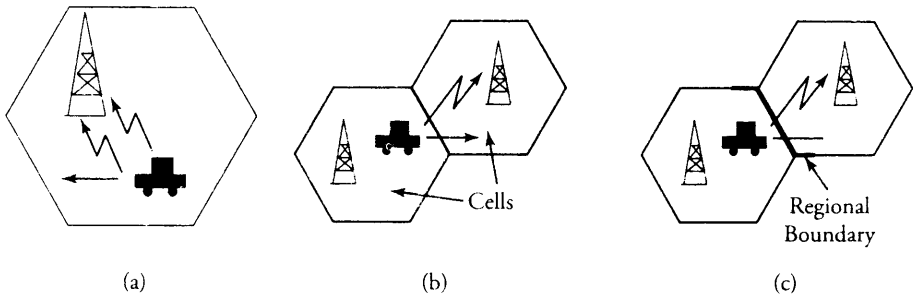


**Figure 6.13** Cellular handoff types: (a) channel handoff, (b) cell handoff, and (c) regional handoff

the base station in a cell, if necessary. If no channels are idle in the cell, the request is rejected, and the wireless terminal has to keep the old channel.

*Cell handoff* occurs between two adjacent cells. When a wireless terminal moves from one cell to another, the handoff request to the new cell is initialized. If no channels are available in the new cell, the handoff call has to be rejected or terminated.

*Regional handoff* occurs when the mobile user moves from one region to another. From a theoretical standpoint, we can model a handoff process between any two regions, using stochastic models. Consider several hexagonal-shaped regions that consist of a group of hexagonal-shaped cells, as illustrated in Figure 6.14. Since the standard of handoff processes is still being developed, we have to assume that only the boundary cells in a region as labeled in Figure 6.14 are involved the regional handoff model. Similarly, when all channels in the new region are in use, all handoff requests have to be rejected.

### 6.4.4 Mobility Management

Mobility management consists of three functions: *location management with user tracking*, *user authentication*, and *call routing*. Location management involves keeping track of the physical location of users and directing calls to correct locations. Before a user's call is routed to the desired location, the user must be authenticated. Routing involves setting up a path for the data directed to the user and updating this path as the user location changes. In cellular networks, *mobile switching centers*, in conjunction with base stations, coordinate the routing and location-management functions.

The requirement for handoff is dependent on the speed of the mobile terminals and the distance between a mobile user and its cell boundaries. The alternation of states for a mobile unit—whether it is still or mobile while carrying a call in progress—also has

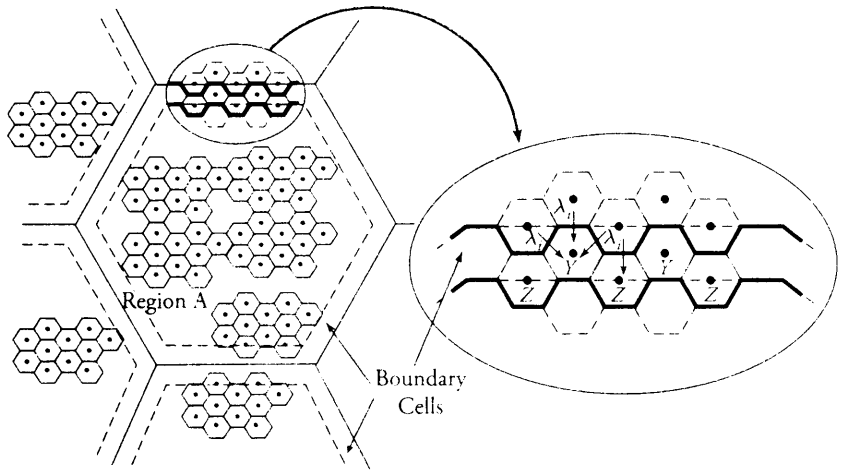


**Figure 6.14** Cellular networks and a regional handoff

to be considered for handoff analysis. In reality, a handoff is needed in two situations: (1) the signal strength within the cell site is low or (2) when a vehicle reaches the cell boundary. We assume that the handoff model is free of signal-strength obstructions. Our second assumption prior to reaching a cell boundary is that a vehicle with a call in-progress alternates between still (stop state) and moving (go-state).

### Stop-and-Go Model

The alternation of stop-and-go states can be modeled, using a simple state machine. In state 0 (stop), a vehicle is at rest but has a call in progress. In state 1 (go), the vehicle moves with an average speed of $k$ mph and has a call in progress. Let $\alpha_{i,j}$ be the rate at which a system with $i$ states moves from state $i$ to state $j$. For example, $\alpha_{0,1}$ is the rate at which state 0 leaves for state 1, and $\alpha_{1,0}$ is the rate at which state 1 leaves for state 0. In our case, it is clear that $\alpha_{0,0} = -\alpha_{0,1}$ and that $\alpha_{1,1} = -\alpha_{1,0}$.

The time in the stop state is an exponential random variable with mean $1/\alpha_{0,1}$ (see Appendix C). The time in the go state also is an exponential random variable, with mean $1/\alpha_{1,0}$. Let $P_i(t)$ be the probability that a vehicle having a call in progress is in state $i$ at time $t$. According to the *Chapman-Kolmogorov* theory on continuous-time Markov chain (explained in Section C.5.1), we can derive

$$P'_j(t) = \sum_i \alpha_{i,j} P_i(t), \tag{6.9}$$

where $P_j'(t)$ is the time differential of relative state $j$ probability. Applying Equation (6.9) for a system with two states, 0 and 1, we have

$$\begin{aligned} P_0'(t) &= \alpha_{0,0}P_0(t) + \alpha_{1,0}P_1(t) \\ &= -\alpha_{0,1}P_0(t) + \alpha_{1,0}P_1(t) \end{aligned} \tag{6.10}$$

$$\begin{aligned} P_1'(t) &= \alpha_{0,1}P_0(t) + \alpha_{1,1}P_1(t) \\ &= \alpha_{0,1}P_0(t) - \alpha_{1,0}P_1(t), \end{aligned} \tag{6.11}$$

where $P_0(t)$ and $P_1(t)$ are the probability that a vehicle having a call in progress is in states 0 and 1, respectively, at time $t$. Knowing that the sum of probabilities is always 1, we get $P_0(t) + P_1(t) = 1$.

This equation and Equation (6.10) can be combined to form a first-order differential equation:

$$P_0'(t) + (\alpha_{0,1} + \alpha_{1,0})P_0(t) = \alpha_{1,0}, \quad P_0(0) = P_0. \tag{6.12}$$

The total solution to the differential equation consists of a homogeneous solution, $P_{0h}(t)$, plus a particular solution, $P_{0p}(t)$. Knowing that $P_{0h}'(t) + (\alpha_{0,1} + \alpha_{1,0})P_{0h}(t) = 0$, where $P_{0h}(0) = P_0(0)$, we can obtain the general solution for Equation (6.12) by

$$\begin{aligned} P_0(t) &= P_{0p}(t) + P_{0h}(t) \\ &= \frac{\alpha_{1,0}}{\alpha_{0,1} + \alpha_{1,0}} + \left( P_0(0) - \frac{\alpha_{1,0}}{\alpha_{0,1} + \alpha_{1,0}} \right) e^{-(\alpha_{0,1}+\alpha_{1,0})t}, \end{aligned} \tag{6.13}$$

where $P_0(t)$ is the probability that a vehicle with a call in progress is in state 0 at time $t$. Similarly, we obtain the general solution for Equation (6.11) by

$$\begin{aligned} P_1(t) &= P_{1p}(t) + P_{1h}(t) \\ &= \frac{\alpha_{0,1}}{\alpha_{0,1} + \alpha_{1,0}} + \left( P_1(0) - \frac{\alpha_{0,1}}{\alpha_{0,1} + \alpha_{1,0}} \right) e^{-(\alpha_{0,1}+\alpha_{1,0})t}, \end{aligned} \tag{6.14}$$

where $P_1(t)$ is the probability that a vehicle with a call in progress is in state 1 at time $t$.

There are four cases for a vehicle to change states.

1. A vehicle is resting permanently but has a call in progress; thus, $P_0(0) = 1$ and $P_1(0) = 0$.
2. A vehicle is moving at an average speed $k$ until it reaches a cell boundary; thus, $P_0(0) = 0$ and $P_1(0) = 1$.

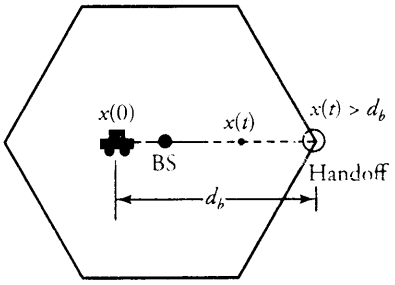


**Figure 6.15** Cellular-handoff model with mobility

3. A vehicle stops at the initial state and moves on a congested path until reaching a cell boundary, so $P_0(0) = 1$ and $P_1(0) = 0$.
4. A vehicle moves and stops on a congested path until reaching a cell boundary; thus, $P_0(0) = 0$ and $P_1(0) = 1$.

Now, consider the mobilized model shown in Figure 6.15. To show the probability of a call to reach a cell boundary with an average speed $k$ m/h with stop and go or the probability of requiring a handoff, let $s$ be the average speed of the vehicle, where $s = 0$ in state 0 and $s = k$ in state 1. Let $x(t)$ be the vehicle's position at time $t$, assuming $x(0) = 0$, and let $d_h$ be the distance a vehicle takes to reach a cell boundary. Suppose that $t$ is a random variable representing a channel holding time, or the time a vehicle takes to reach a cell boundary. Let $P_i(t, d_h)$ be the probability that a vehicle in state $i$ with a call in progress is at the cell boundary at time $t$, where $i \in \{0, 1\}$. Consequently, the probability that a vehicle reaches a cell boundary with speed $s$ undergoing stop-and-go states is

$$P[x(t) \geq d_h] = P_0(d_h/s, d_h)\Big|_{s=0} + P_1(d_h/s, d_h)\Big|_{s=k}, \tag{6.15}$$

where

$$P_0(d_h/s, d_h)\Big|_{s=0} = \frac{\alpha_{1,0}}{\alpha_{0,1} + \alpha_{1,0}} \tag{6.16}$$

and

$$P_1(d_h/s, d_h)\Big|_{s=k} = \frac{\alpha_{0,1}}{\alpha_{0,1} + \alpha_{1,0}} + \left(P_1(0) - \frac{\alpha_{0,1}}{\alpha_{0,1} + \alpha_{1,0}}\right) e^{-(\alpha_{0,1}+\alpha_{1,0})d_h/k}. \tag{6.17}$$

In case 1, since a vehicle is resting all the time, with an average speed of 0 m/h, the probability of reaching a cell boundary is clearly 0 percent. In contrast, for a vehicle moving with an average speed ($k$) (case 2), the chance of reaching a cell boundary is always 100 percent. Thus, when a vehicle is either at rest or moving, the probability of requiring a handoff is independent of $d_h$.

### 6.4.5 Generations of Cellular Systems

First-generation cellular systems were mostly analog. Channels were allotted to a single user, and each user had dedicated access to the channel. This led to underutilization of resources. Second-generation systems were digital and supported higher data rates, providing digital traffic channels and digitized voice before transmission over the channel. Data digitization made it simple to implement an encryption scheme. The digital traffic also made it possible to deploy better error detection and correction. Finally, multiple users shared a channel by using multiple-access schemes, such as TDMA or CDMA.

Third and later generations of wireless networks provide high data rates and support multimedia communications, in addition to voice communications. The main objectives for these cellular networks are to achieve quality voice communications, higher data rates for stationary and mobile users, support for a wide variety of mobile devices, and adapting to new services and technology usable in a wide variety of environments, such as offices, cities, and airplanes. Design issues involved the design of CDMA-based systems are *channel-usage bandwidth limitation* (5 MHz), *chip rate*, and multirate capability to provide different data rates on different channels for each user. The multirate scheme can scale effectively to support multiple applications from each user.

### 6.4.6 CDMA-Based Mobile Wireless

The most commonly used second-generation CDMA scheme is IS-95, which consists of two components: a *forward link* and a *reverse link*. The forward link consists of 64 CDMA channels, each operating at a bandwidth of 1.288 MHz. The channels are of four types:

1. *Pilot channel* (channel 0). This channel helps a mobile user to obtain timing information and enables the mobile unit to track signal-strength levels to initiate handoffs.
2. *Synchronization channel* (channel 32). This channel operates at 1,200 b/s and helps a mobile user to obtain information, system time and protocol version, from the cellular system.

3. *Paging channels* (channels 1–7). These channels are used for monitoring paging requests.
4. *Traffic channels* (channels 8–31 and 33–63). The forward link supports up to 55 traffic channels supporting data rates of up to 9,600 b/s.

If the data rate is low, bits are replicated to increase the rate to 19.2 Kb/s. This process, called *symbol repetition*, is followed by a scrambling process for increasing privacy and reducing the interference between users. The next step is a process to control the power output of the transmitting antenna. The data is then processed, using *direct-sequence spread spectrum* (DSSS) (see Chapter 4). This process spreads the transmitted signal from 19.2 Kb/s to 1.288 Mb/s. The *Walsh matrix* is used to generate the pseudorandom sequence. The signal is then modulated with the QPSK modulation scheme being transmitted onto the medium.

The *IS-95 reverse link* consists of up to 94 CDMA channels, each operating at 1.228 MHz. The link supports up to 32 access channels and 62 traffic channels. The access channels are used for call setup, location update, and paging. The reverse-link transmission process is very similar to forward-link transmission. The convolution encoder has a rate of 0.333. Thus, the data rate is tripled, to $3 \times 9.6 = 28.8$ Kb/s, followed by the data-scrambling process achieved by block interleaving. In the reverse link, the Walsh matrix is used to increase the data rate to 307.2 Kb/s as the data from the block interleaver is divided into 6-bit units to improve reception at the receiver. The data-burst randomizer is used in conjunction with the long code mask to reduce interference from other users. In the case of the reverse link, the long code mask is unique for each mobile unit. The resultant data is modulated, using the orthogonal QPSK modulator (OQPSK). The OQPSK scheme is used because the spreading codes need not be orthogonal for the reverse link.

**Example.** Consider a voice signal. It is first digitized at 8,500 b/s. Then error detection is added, which increases the number of bits and hence the data rate to around 9,600 b/s. During the idle periods of a conversation, the data rate can be lowered to around 1,200 b/s. The digitized voice signal is now transmitted in blocks of 20 ms interval. Forward error correction is provided by using a convolution encoder with rate of 0.5. This increases the data rate to $2 \times 9.6 = 19.2$ Kb/s.

## 6.5 Mobile IP

The *mobile IP* scheme is a protocol responsible for handling the mobility of users attached to the Internet. *Mobile computing* allows computing devices, such as computers, to move while functioning routinely. In a mobile IP network, it is essential for both

mobile and wired users to interoperate seamlessly. In most mobile IP cases, TCP cannot be used, as the congestion-control scheme would greatly reduce the throughput and the inherent delays and error bursts may result in a large number of retransmissions. Some changes have to be made to TCP to use it for internetworking wired and wireless networks. The major challenges with mobile IP are

- *Mobility*. A quality connection is desired for a user while it is mobile with different speeds.
- *Registration*. A mobile user's address must be identified and registered in different areas.
- *Interoperability*. A mobile user must interact with other stationary and mobile users.
- *Connection reliability*. TCP connections must survive in mobility cases.
- *Security*. A connection must be secured, especially since a wireless connection is less immune to intrusions.

A mobile user requires the same level of reliability for a TCP connection as he/she receives in a wired connection. Note that, typical Internet congestion-control schemes cannot be used in wireless networks, because the packet drop is caused mainly by poor link quality and channel distortions rather than by congestion. The channel imperfections make it difficult to implement a quality-of-service model other than the best-effort model. The varying data rates and delays make it challenging to implement high-speed and real-time applications, such as voice and video, over wireless networks.

### 6.5.1 Addresses and Agents

In a mobile IP network, a mobile host (mobile user) is allowed to hold two addresses simultaneously. One of the two addresses is permanent and the other is temporary. The permanent address of a host is the conventional IP address. Note that similar to regular networks, there are still MAC (at the link-layer) addresses in wireless networks that identify physical endpoints of links. A mobile host must have a permanent IP address in its *home network*. This address is called the *home address*. A home address is an IP address and is assigned to a mobile host for an extended period of time. The home address remains unchanged even if the host moves out of its home area. In such cases, a host needs to be registered by the home *mobile switching center* (MSC). This MSC is a router and it iss called the *home agent*.

When a mobile host leaves its home network and enters a *foreign network*, the host must also be registered by the new network and obtain a temporary address. Changing

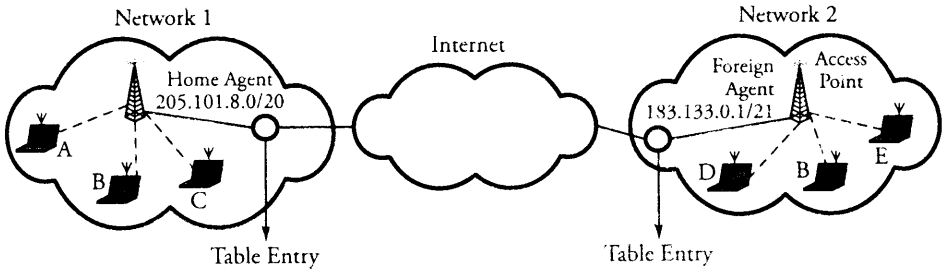


Table Entry

| Mobile Host | Home IP Address | Foreign IP Address |
|---|---|---|
| A | 205.101.8.5 | ... |
| B | 205.101.8.3 | 183.133.0.1 |
| C | 210.43.12.78 | 205.101.8.28 |

Table Entry

| Mobile Host | Home IP Address | Foreign IP Address |
|---|---|---|
| D | 183.133.0..5 | 143.156.7.43 |
| E | 183.133.0..28 | ... |
| B | 205.101.8.3 | 183.133.0.1 |

**Figure 6.16** A mobile host moves from its home network to a foreign network

the network typically happens when a mobile host roams in a certain city or changes the city. Once a mobile host leaves its home network for a foreign network, it is assigned a *foreign address* reflecting the mobile host's current point of attachment when away from its home network. In such a case, its messages from the Internet corresponding servers are still sent to the mobile's home address. Similarly, a *foreign agent* is a router in the mobile host's foreign network that informs a host's home agent of its current foreign address. The home agent always forwards messages to the mobile host's current location. Figure 6.16 shows two wireless networks attached to the Internet in which mobile host B has moved from its home network to a foreign network.

Generally, MSC routers (acting as agents) in a network are connected through high-speed links to all access points (base stations) in a network. An MSC router maintains two databases: a home-location database and a foreign-location database. When a mobile host moves to its home network, a signal is sent to the local base station which forwards this signal to its MSC. The MSC router in turn authenticates the user and registers the user in its home-location database.

## 6.5.2 Agent Discovery Phase

A home agent maintains a database containing the mobile host's home address. When a mobile host moves to a foreign network, its home and foreign agents establish an association for updating registration with its home agent through the foreign agent. This association is made possible by sending agent advertisement messages. Upon receiving an agent advertisement, the mobile host can learn if it is located in its home network

or in a foreign network depending on the type of message. A mobile host can detect if it is connected to its home link or foreign link. Once the host moves to a new network, it can determine whether it has changed its point of attachment to obtain a foreign address.

Advertisement messages are propagated periodically in a broadcast manner by all agents. It is always possible that a mobile host does not receive the advertisement due to restricted timing. In such a case, the mobile host needs to send a request message to the agent which it is attached to. If the agent to which the host is attached is a home agent, the registration process is the same as traditional host in a fixed place. But, if the agent is a foreign one, the agent replies with a message containing a foreign address for the agent.

### 6.5.3 Registration

Mobile IP acts as an interface between the mobile's home network and the foreign network where the mobile currently resides. Mobile IP keeps track of the mobile's locations, and maps a home address into a current foreign address. The mobile IP interface delivers messages from the mobile's home network to the mobile host in its current foreign location in a seamless fashion after a registration process with the foreign agent is completed. The procedure of registration with a new network is summarized as follows:

**Mobile IP Registration Steps**

1. Use UDP (a transport layer protocol to be discussed in Chapter 8) and register with an agent on the new network
2. On the home network, register with an agent to request call forwarding
3. If any registration is about to expire, renew it
4. When returning to the home network, cancel the registration with the new network.

■

A registration phase involves an exchange of two messages between the mobile host and its home agent: *registration request* and *registration response*. Once a mobile host enters a foreign network, it listens for agent advertisements and then obtains a foreign address from the foreign network it has moved to. The host's home-network agent then adds the foreign network address agent to its home-location database. This is done after the agent authenticates the host through the host's home-network agent. The host's home-network agent now forwards all calls to the host in the foreign network. On the Internet, the location management and routing are done through mobile IP.

A mobile host can also register using a *collocated foreign address*. A collocated foreign address is a local IP address temporarily assigned to a mobile host without using a foreign agent. In a collocated foreign addressing, a mobile host receives an assigned temporary foreign address through its own home network. In the meanwhile, as soon as the mobile host leaves the foreign network, it also requires to deregister.

**Example.** Consider Figure 6.16 showing two wireless networks connected to the Internet. Network 1 is assigned a CIDR IP address (see Chapter 2) 205.101.8.0/20 and it has three active mobile hosts A, B, and C. Suppose that this network is the home network for hosts A and B and but not for host C as it appears from the home IP addresses of the agent routing entry. Consider a situation in a different time in which host A stays in this network (thus there is no foreign address for it), and host B moves out of this network (thus it obtains a foreign address). Particularly, host B has moved to network 2. Network 2 is also assigned a CIDR IP address 183.133.0.1/21 and it has three active mobile hosts D, E, and B. Network 2 is now considered a foreign network for B and is therefore assigned a foreign address of 183.133.0.1. This address appears in its both associated home and foreign agents as seen in the figure.

## 6.5.4 Mobile IP Routing

In mobile IP systems, datagrams are encapsuled by a mobile IP header. Figure 6.17 shows the header format of mobile IP registration. The *type* field determines whether the registration is a request or a reply. The *flags/code* field is used in the reply-message to specify forwarding details. The *lifetime* field gives the permitted time (in seconds) a registration is valid. The home address and *temporary address* fields are the two addresses explained. The *home agent* field specifies the home-agent address of the host. The *identification* field helps a mobile host prevent repeated messages.

Each datagram forwarded to the mobile host's home address is received by its home agent, and then it is forwarded to the mobile host's foreign address. In this case, mobile host's foreign agent receives the datagram and forwards it to the mobile host. If a mobile

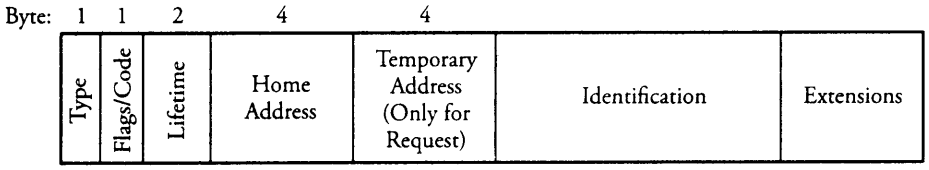


**Figure 6.17** Header format of mobile IP registration

host residing in a foreign network wants to send a message to host outside of its new network, the message is not required to be passed through its home agent. In such a case, the message is handled by the foreign agent.

Mobile IP has two routing schemes: *Delta routing* and *direct routing*. In the Delta routing, a triangular path is established among the host's home agent, host's foreign agent, and a corresponding machine. Suppose that the mobile host belonging to wireless network 1 moves to foreign network 2. While in the foreign network, the mobile host is contacted for communication by a server (as a corresponding machine) fixed in a residential area network. In this case, a datagram (IP packet) from the server is first sent to the mobile's home network using standard IP routing. The host's home agent detects the message, finds the host's foreign address, and forwards the message to the host's foreign agent. The foreign agent delivers the message to the mobile host. In response, the mobile host can send its reply directly to the server through the foreign agent. This routing process forms a triangular-shape path routing and that is why it is called Delta routing.

Now, consider a case that a mobile host is the one who wants to initiate the transmission of a message with a server in the same scenario as explained above. In the first step, the mobile host informs the server of its foreign address. Then, the mobile host can send the message directly to the server through its foreign agent bypassing its home agent. This way a chunk of signaling due to routing to home agent is eliminated. We remember that the corresponding server should initiate a communication with a mobile host always starting to contact the mobile host's home agent since the server does not have a real-time knowledge of the mobile host's whereabout.

As we see, the routing of mobile users may involve many different challenges. For example, in the previous scenario, if the mobile host moves to yet a new foreign network, say network 3. In this case, the mobile host can inform its previous foreign agent about its new foreign address, so that datagrams (IP packets) routed to the old location can now be routed to the new foreign location.

### Virtual Registration and Routing

In order to reduce the cost and the amount of registration with the home agent, the mobile Internet protocol also offers facility called *virtual registration*. In each region, *virtual agents* instead of just a home agent can be defined. Virtual regions are then defined based on statistics and the density of traffic. Each virtual agent covers services over a local virtual region. When a mobile host enters the virtual region, it registers with the virtual agent. Thus, in a scenario of routing messages between a mobile host and a corresponding server described in the previous section, datagrams from

the corresponding server are sent to the mobile's home address, and then routed to the mobile's foreign address. Datagrams are then sent from the home agent to the virtual agent first and, from there, to the foreign agent. In such cases, the mobile host has typically no knowledge of the network for routing decision making.

### Tree-Based Routing

The amount of registration between a home network and a foreign network can also be reduced by a carefully designed hierarchy of foreign agents. In a hierarchical structure, multiple foreign agents are advertised in the agent advertisement. With this scheme, a mobile host has to configure to what upper level at the tree its new registration has to go. The mobile host should then transmit the registration to each level of the hierarchy between itself and the closest common parent between its new and previous foreign addresses. If a mobile host currently using the services of one foreign agent moves to a different foreign agent, it may not involve a direct registration with its home agent.

Figure 6.18 shows a tree-based hierarchy of foreign agents. Suppose that a mobile host is currently using the service of foreign agent A16 while at location L1. The mobile host receives agent advertisements from foreign agents A1, A2, A4, A7, A11, and A16. Registration messages are sent to each of these foreign agents and its home agent. However, the home agent of the mobile host can only identify foreign agents in its outside world as far as to foreign agent A1. This means that, the topology of the hierarchy beyond A1 may stay unknown for the home agent even though it receives messages from other agents. The same thing is true for agent A1 which can see only up to its nearest neighbors A2 and A3, and so on for others. In fact, no agent knows exactly where the mobile host is located except for foreign agent A16.

When the mobile host moves to the vicinity of foreign agent A17 at location L2, the host needs a new registration valid to travel upto the vicinity of A11. If the mobile moves to the vicinity of foreign agent A19 at location L3, the situation is different as A17 and A19 are linked directly to a common node as was the case for A16 and A17. In this case, the mobile host receives advertisements specifying the hierarchy of A4, A8, A13, and A19. The mobile host then compares the previous hierarchy and this new one and determines that it has caused the registration to move to as high as level A4 in the tree-based scheme. The same procedure occurs when the mobile host decides to move to location L4.

### Mobile Routing with IPv6

Mobile IPv6 offers a simpler mobile routing scheme. With IPv6, no foreign agent is required. A mobile host should use the *address autoconfiguration procedure* embedded

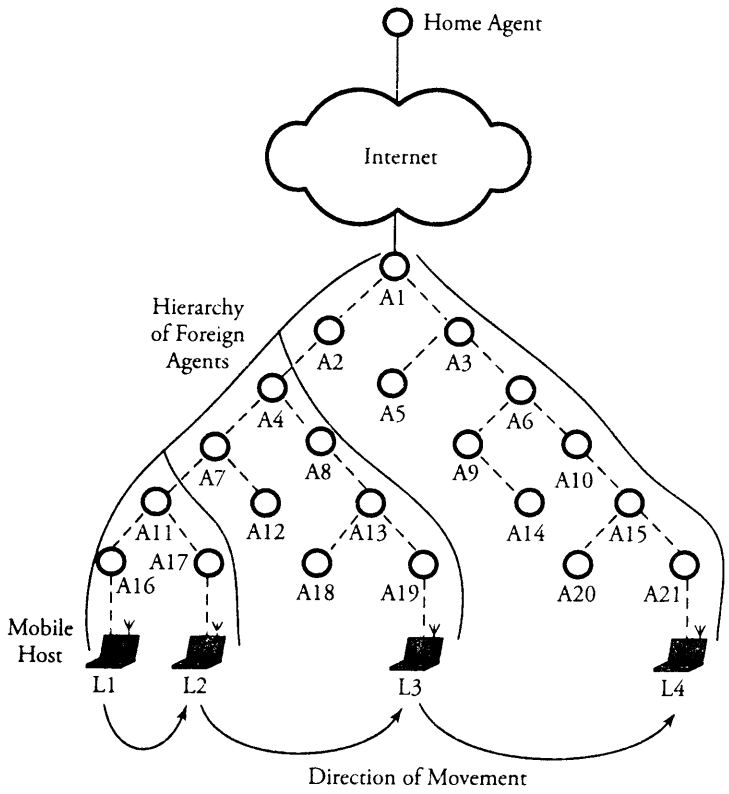


**Figure 6.18** Routing in a tree-based structure of foreign agents

in IPv6 to obtain a foreign address on a foreign network. The procedure to route with mobile IPv6 is summarized as follows:

### Mobile IPv6 Routing Steps

1. A host informs its home agent and also corresponding machines about its foreign address.
2. **If** a corresponding machine knows the mobile's current foreign address, it can send packets directly to the mobile host by using the IPv6 routing header; **Otherwise** the corresponding machine sends packets without the IPv6 routing header.
3. Packets are routed to the mobile host's home agent
4. Packets are forwarded to the mobile host's foreign address
5. **If** the mobile host moves back to its home network, the host notifies its home agent. ■

It is clear that the routing steps are similar to IPv4 ones except for the elimination of foreign agent in IPv6. Overall, routing with IPv6 is simpler and the option of source routing is also available.

### 6.5.5 Security

Wireless links are susceptible to eavesdropping or passive traffic monitoring. The inherent broadcast paradigm in wireless networks make them more susceptible to various attacks. The security for these networks involve:

- Network security
- Radio link security
- Hardware security

Radio link security involves preventing the interception of radio signals, defense against jamming attacks, and encrypting traffic to ensure privacy of user location. The security portion of wireless system must prevent the misuse of mobile units by making them tamper resistant. The hardware component of wireless security is especially complex. The details of security in wireless networks are discussed in Chapter 10.

## 6.6 Wireless Mesh Networks (WMNs)

A *wireless mesh network* (WMN) is a dynamically self-organized wireless network that maintains *mesh* connectivity. WMNs help users stay online anywhere, anytime, for an unlimited time. One key component that makes this happen is the type of wireless router used in mesh infrastructures. We look at applications of WMNs, and WiMax networks, the conductivities of P2P networks with backbone wireless mesh networks.

### 6.6.1 WiMAX Technology and IEEE 802.16

The *worldwide interoperability for microwave access* (WiMAX) technology is a certification mark for the IEEE 802.16 standard. This standard is implemented for point-to-multipoint broadband wireless access. WiMAX is a wireless WAN technology that can connect IEEE 802.11 WiFi hotspots with one another and to other parts of the Internet. WiMAX also provides a wireless alternative to cable and DSL for broadband access. WiMAX devices are capable of forming wireless connections to allow Internet packets to be carried across a network. Conceptually, WiMAX is similar to WiFi technology but has been improved for use over much greater distances.

The IEEE 802.16 standard offers a significant improvement for communications, as it defines a MAC layer that supports multiple physical-layer specifications, potentially making WiMAX a great framework for wireless broadband communications. The 802.16 MAC is a scheduling MAC whereby the user device competes once for initial entry into the network. After being in the network, the base station allocates a time slot to the user. This time slot can enlarge or constrict, and no other users can use it. Unlike 802.11, the 802.16 scheduling algorithm exhibits stability given overload and offers better bandwidth efficiency. Another advantage is that 802.16 lets the base station offer QoS by balancing the assignments of users.

The IEEE 802.16 standard has determined the frequency range of 10 GHz to 66 GHz. WiMAX improves on the WiFi standard by providing increased bandwidth and stronger encryption. WiMAX makes excellent use of multipath signals. IEEE 802.16 dictates up to 50 km of connectivity services between users without a direct line of sight. This does not mean that a user 50 km away with no line of sight has connectivity, and practically, this distance is 5 km to 8 km. The data rate with WiMAX is up to 70 Mb/s, which is sufficient to simultaneously support more than 60 businesses with T-1-type connectivity. The line of sight is about 1,000 homes at 1 Mb/s DSL-level connectivity.

WiMAX antennas can share a cell tower without impacting the normal operations of the cellular network. A WiMAX antenna can even be connected to an Internet backbone via optical fibers or directional microwave link. WiMAX may be considered for cities or countries willing to skip a wired infrastructure, establishing a wireless infrastructure in an inexpensive, decentralized, deployment-friendly, and effective manner.

## 6.6.2 Applications of Mesh Networks

In WMNs, two types of nodes perform the routing: *mesh routers* and *mesh users*. Figure 6.19 shows detailed connectivity of a backbone mesh network to WiFi, WiMAX, and wireless cellular networks. In this figure, a WiFi network, a cellular network, and a WiMAX network are connected through mesh routers with *gateway bridges*. A router with gateway bridge capability enables the integration of WMNs with other type networks, although traditional routers with regular *network interface cards* (NICs) can connect to mesh networks.

Mesh users can also operate as routers for mesh networking, making the connectivity much simpler and faster than conventional wireless networks with base stations. Figure 6.20 shows another scenario, in which a wireless mesh network backbone is connected to wireless mesh users. Users are communicating in an ad hoc fashion, with each individual user acting as a router and connected to a mesh router gateway. In this

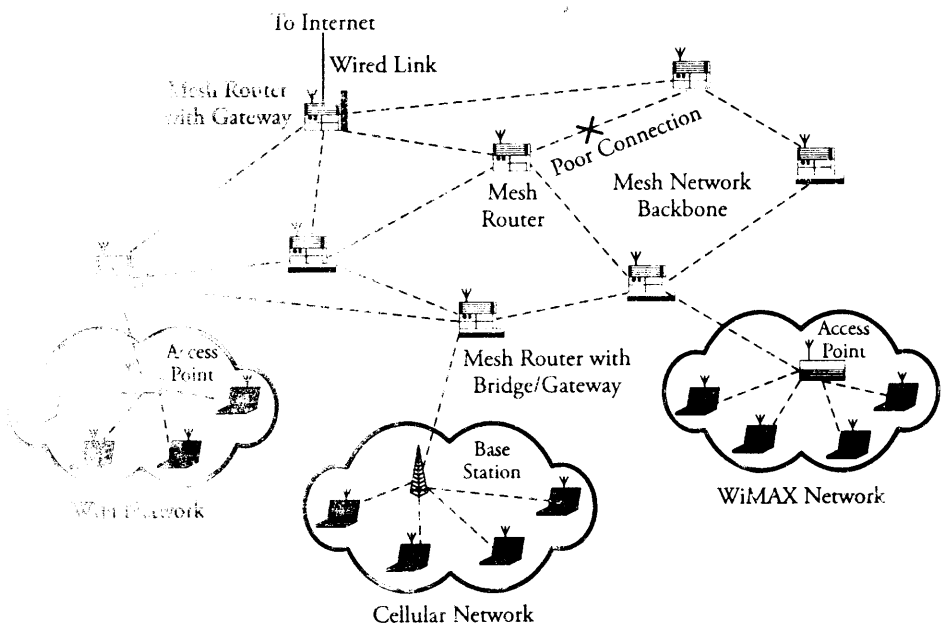


Figure 6.13 Overview of a backbone mesh network and connections to WiFi, WiMAX, and wireless cellular networks

network. Wired users, as shown by a LAN in the figure, can also be connected to WMN, using a mesh router gateway. User meshing provides *peer-to-peer* networks among users (discussed in Chapter 16).

The inclusion of multiple wireless interfaces in mesh routers significantly enhances the capability of mesh networks. WMNs offer advantages of low cost, easy network maintenance, and remarkably more reliable service coverage than conventional ad hoc networks. Mesh networks are being designed for metropolitan and enterprize networking, and most of standards, such as IEEE 802.11, IEEE 802.15, and IEEE 802.16, are adopted in WMN infrastructures. A widely accepted radio technology is the series of IEEE 802.11 standards.

The benefits of a mesh network are as follows:

- *Scalability*. The WMN infrastructure is designed to be scalable as the need for network access increases.
- *Ad hoc networking support*. WMNs have the capability to self-organize and be connected to certain points of ad hoc networks for a short period of time.

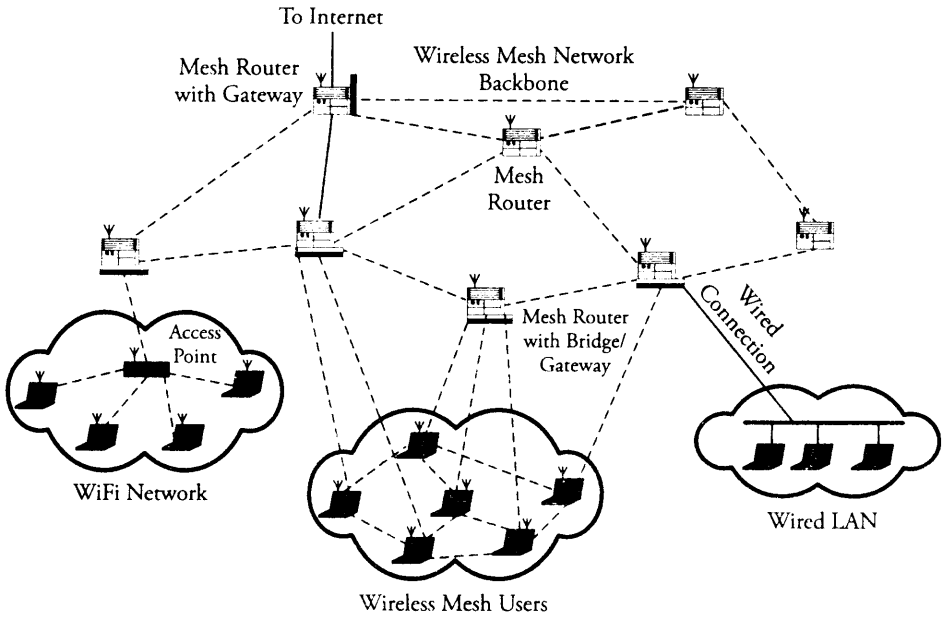


**Figure 6.20** Connectivity between a backbone wireless mesh network to wireless users and other networking devices

- *Mobility support of end nodes.* End nodes are supported through the wireless infrastructure.
- *Connectivity to wired infrastructure.* Gateway mesh routers may integrate heterogeneous networks in both wired and wireless fashions.

To achieve scalability in WMNs, all protocols—from the MAC layer to the application layer—must be scalable. "Topology-" and "routing-aware" MAC can substantially improve the performance of WMNs.

The QoS provisioning in wireless mesh networks is different from that of classical ad hoc networks. Several applications are broadband services with heterogeneous QoS requirements. Consequently, additional performance metrics, such as delay jitter and aggregate and per node throughput, must be considered in establishing a route. Application-specific security protocols must also be designed for WMNs. Security protocols for ad hoc networks cannot provide any reliability, as the traffic in such networks can resemble the one flowing in the wired Internet.

### 6.6.3 Physical and MAC Layers of WMNs

The *physical layer* of wireless mesh networks benefits from existing modulation and coding rates. *Orthogonal frequency multiple access* (OFDM) and *ultrawide band* (UWB) techniques are used to support high-speed wireless communications.

#### Physical Layer

WMN communication quality and system capacity have been improved through the use of multiantenna systems, such as antenna diversity, smart antenna, and MIMO (*multiple-input multiple-output*) systems. MIMO algorithms send information over two or more antennas. The radio signals reflect objects, making multiple paths that in conventional radios cause interference and fading. A MIMO system uses these paths to carry more information. Another improvement in WMNs includes the use of *cognitive radios*, which dynamically capture unoccupied spectrum. One of the unique features of this technology is that all components of its radio, including RF bands, channel-access modes, and even channel modulations, are programmable.

#### MAC Layer

The WMN MAC layer is different from classical wireless networks. In WMNs, the MAC layer

1. Is designed to face more than one-hop communication
2. Is distributed to support multipoint-to-multipoint communications
3. Has self-organization features
4. Has moderately lower mobility than in classical wireless networks

Wireless mesh MAC protocols can be designed for both a single channel or multiple channels or to even operate simultaneously. A multiple-channel MAC setup improves network performance significantly by increasing network capacity. Because of the poor scalability of CSMA/CA schemes, these techniques are not efficient solutions for single-channel MAC protocols. The best solution for WMNs is the enhanced versions of TDMA or CDMA, owing to low complexity and cost.

Multichannel MACs can be deployed in various ways. With *multichannel single-transceiver* MAC, only one channel can be active at a time in each network node, as only one transceiver is available. With *multichannel multitransceiver* MAC, several channels can be active simultaneously and only one MAC-layer module is assigned to coordinate all channels. With *multiradio* MAC, each node has multiple radios, and each radio has its own MAC layer and physical layer.

## 6.7 Summary

This chapter presented basics of wireless networking without touching on the large-scale routing issues. Starting with the fundamental concept at the LAN level, we analyzed several IEEE 802.11 standards. The basic versions—802.11a, 802.11b, and 802.11g—typically use *Carrier Sense Multiple Access* with *collision avoidance* (CSMA/CA).

A *cellular network*, includes a networked array of *base stations*, each located in a hexagonal *cell* to cover networking services. Each mobile user should register with the regional *mobile switching center*. Because of unexpected interference whenever a user works with radio frequencies, we looked at known interference and *frequency reuse*. Frequency reuse in a certain region of a wireless network occurs when the same frequency used in one area could be reused to cover another area.

We also studied *mobile IP*. We learned that this protocol is responsible for handling the mobility of users attached to the Internet. A mobile host is allowed to hold two addresses simultaneously: a home address and a foreign address. One of the main elements of mobile IP is registration in a foreign network.

At the end of this chapter, we introduced *wireless mesh networks* (WMNs), including WiFi and WiMAX technologies. The *wireless fidelity* (WiFi) technology is a set of standards for wireless local area networks that allows mobile devices, such as laptop computers, digital cameras, and personal digital assistants, to connect to local area networks. The *world wide interoperability for microwave access* (WiMAX) technology is the IEEE 802.16 standard that can connect IEEE 802.11 WiFi hotspots to one another and to other parts of the Internet. We also looked at *wireless mesh networks* (WMNs) constructed as a wireless network backbone for several applications.

In the next chapter, we study routing and internetworking issues in widearea networks. We explore how routing algorithms and protocols are performed both within and beyond a single wide area network.

## 6.8 Exercises

1. Consider a commercial wireless mobile telephone system whose transmitter and receiver are located 9.2 km apart. Both use isotropic antennas. The medium through which the communication occurs is not a free space, and it creates conditions such that the path loss is a function of $d^3$ and not $d^2$. Assume that the transmitter operating at the frequency of 800 MHz communicates with a mobile receiver with the received power of $10^{-6}$ microwatts.
   (a) Find the effective area of the receiving antenna.
   (b) Find the required transmission power.

2. Assume that cellular networks were modeled by square cells
   (a) Find the cell coverage area, and compare it to the one using hexagonal cells. Assume that the distance between the cell centers are identical in these two models.
   (b) What are the disadvantages of this model compared to the one with hexagonal cells?

3. A cellular network over 1,800 $km^2$ supports a total of 800 radio channels. Each cell has an area of 8 $km^2$.
   (a) If the cluster size is 7, find the system capacity.
   (b) Find the number of times a cluster of size 7 must be replicated to approximately cover the entire area.
   (c) What is the impact of the cluster size on system capacity?

4. Consider a cellular network with 128 cells and a cell radius $r$=3 km. Let $g$ be 420 traffic channels for a $N = 7$-channel cluster system.
   (a) Find the area of each hexagonal cell.
   (b) Find the total channel capacity.
   (c) Find the distance between the centers of nearest neighboring cochannel cells.

5. If cells split to smaller cells in high-traffic areas, the capacity of the cellular networks for that region increases.
   (a) What would be the trade-off when the capacity of the system in a region increases as a result of cell splitting?
   (b) Consider a network with 7-cell frequency reuse clustering. Each cell must preserve its base station in its center. Construct the cell-splitting pattern in a cluster performed from the center of the cluster.

6. We would like to simulate the mobility and handoff in cellular networks for case 4 described in this chapter. Assume 25 mph $\leq k \leq$ 45 mph within city and 45 mph $\leq k \leq$ 75 mph for highway. Let $d_b$ be the distance a vehicle takes to reach a cell boundary, ranging from $-10$ miles to 10 miles.
   (a) Plot the probability of reaching a cell boundary for which a handoff is required. Discuss why the probability of reaching a boundary decreases in an exponential manner.
   (b) Show that the probability of reaching a cell boundary for a vehicle that has a call in progress is dependent on $d_b$.
   (c) Show the probabilities of reaching a cell boundary as a function of a vehicle's speed.

(d) Discuss why the probability of reaching a cell boundary is proportional to the vehicle's speed.

7. *Computer simulation project*. Consider again the mobility in cellular networks for case 4 described in this chapter, but this time, we want to simulate the handoff for three states: stop, variable speed, and constant speed. For the variable-speed case, assume that the mobile user moves with a constant acceleration of $K_1$ m/h. Assume 25 m/h $\leq k \leq$ 45 m/h within city and 45 m/h $\leq k \leq$ 75 m/h for highway. Let $d_b$ be the distance a vehicle takes to reach a cell boundary, ranging from $-10$ miles to 10 miles.
   (a) Plot the probability of reaching a cell boundary for which a handoff is required. Discuss why the probability of reaching a boundary decreases in an exponential manner.
   (b) Show that the probability of reaching a cell boundary for a vehicle that has a call in progress is dependent on $d_b$.
   (c) Show the probabilities of reaching a cell boundary as a function of a vehicle's speed.
   (d) Discuss why the probability of reaching a cell boundary is proportional to the vehicle's speed and that the probability of requiring a handoff decreases.

CHAPTER 7

# Routing and Internetworking

This chapter focuses on the networking structure of larger networks. One of the most important functions in computer networking, especially in wide area networks, is *routing* packets. In packet-switched networks, this function includes procedures through which a packet uses certain algorithms to find all the necessary paths from its source to its destination. In this chapter, we look at routing algorithms and protocols both within one WAN (*intradomain networking*, or *intranetworking*) and beyond it (*interdomain networking*, or *internetworking*). This chapter covers the following main topics:

- *Network-layer routing*
- *Classification of routing algorithms:*
  - *least-cost-path algorithms*
  - *non-least-cost-path routing*
  - *intradomain routing protocols*
  - *interdomain routing protocols*
- *Network-layer congestion control*

We begin with some basic material about routing, such as the definition of path cost and the classification of routing algorithms. A networking infrastructure deploys a variety of algorithms for routing packets, classified as those using optimal routes and those using nonoptimal routes. We also classify routing protocols by whether they are applied within a domain or beyond a domain.

We also look at congestion-control mechanisms that can be implemented either unidirectionally or bidirectionally among nodes at the network layer. At the end of the discussion on congestion control, an approximation method for calculating *link blocking* is introduced. This method provides a quick approximation method for the performance evaluation of links.

## 7.1 Network-Layer Routing

*Routing algorithms* create procedures for routing packets from their sources to their destinations. Routers are responsible mainly for implementing routing algorithms. These routing tasks are essentially methods of finding the best paths for packet transfer in a network. The choice of routing protocol determines the best algorithm for a specific routing task. As seen in Figure 7.1, a host and a server are two end points connected through routers R4, R7, and R1. Each end point belongs to a separate LAN. In such scenarios, a layer 3 (network) route must be set up for IP packets (datagrams); all devices, including end users and routers, process the route at the third layer of the protocol stack, as shown in the figure.

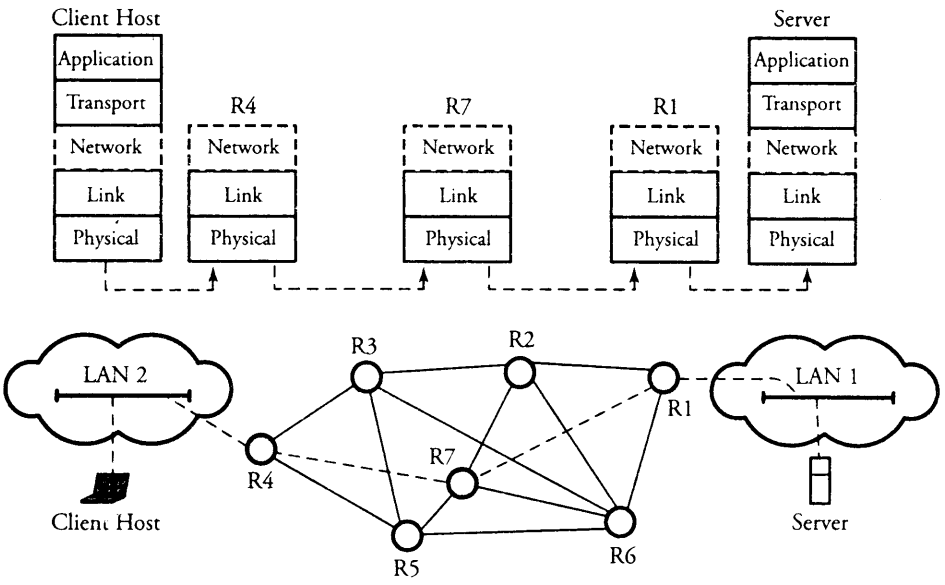


**Figure 7.1** End-to-end communication between a client host and a server at the network layer

Routing algorithms can be differentiated on several key characteristics:

- *Accuracy*. An algorithm must operate correctly so that it can find the destination in an appropriate amount of time.
- *Simplicity*. Low complexity of algorithms is particularly important where routers with limited physical resources involve software.
- *Optimality*. This refers to the ability of the routing algorithm to select the best route.
- *Stability*. Routing algorithms must perform correctly in the face of unforeseen circumstances, such as node failure and routing table corruptions.
- *Adaptability*. When a failure happens in a network, an algorithm should be able to adapt load increases or decreases.
- *Convergence*. Routing algorithms must converge rapidly when a network distributes routing update messages.
- *Load balancing*. A good routing algorithm balances over eligible links to avoid having a heavily and temporarily congested link.

In practice, this list is used to determine how efficiently a route is selected. The first factor to account for determining the best path to a destination is the volume of traffic ahead.

### 7.1.1 Assigning Addresses to Hosts and Routers, and DHCP

Suppose that LAN 1 in Figure 7.1 has an Internet service provider denoted by ISP 1 and that LAN 2 has an ISP denoted by ISP 2. Assume that ISP 1 handles the LAN 1 networking tasks of two independent local departments with IP address blocks 205.101.8.0/23 and 205.101.10.0/23, respectively. Similarly, ISP 2 handles the LAN 2 networking tasks of two independent local departments with IP address blocks 145.76.12.0/22 and 145.76.14.0/22, respectively. (Recall from Chapter 2 the CIDR IP addressing scheme being used here.)

In this scenario, ISP 1 clearly advertises to its outside domains through router R1 that it can process any datagram (IP packet) whose first 22 address bits exactly match 205.101.8.0/22. Note that the outside domains need not know the contents of these two address blocks, as the internal routing within each LAN is handled by an internal server. Similarly, ISP 2 advertises to its outside domains through router R4 that it can process any datagram whose first 21 address bits exactly match 145.76.12.0/22. If for

any reason ISP 1 and ISP 2 merge, the least costly solution to avoid changing the address blocks of ISPs is to keep all address blocks unchanged and to have both R1 and R2 advertise to their outside domains that each can process any datagram whose first 22 address bits exactly match 205.101.8.0/22 or whose first 21 address bits exactly match 145.76.12.0/22.

IP addresses are organized by the *Internet Corporation for Assigned Names and Numbers* (ICANN). An ISP can request a block of addresses from ICANN. Then, an organization can also request a block of addresses from its ISP. A block of addresses obtained from an ISP can be assigned over hosts, servers, and router interfaces by a network manager. Note that always a unique IP address must always be assigned to each host as client or server or router interface (input port or output port). However, under some circumstances, a globally unique IP address assignment can be avoided (Section 7.1.2).

#### Dynamic Host Configuration Protocol (DHCP)

A different method of assigning addresses to a host is called *Dynamic Host Configuration Protocol* (DHCP), whereby a host is allocated an IP address automatically. DHCP allows a host to learn its subnet mask, the address of its first-hop router, or even the address of other major local servers. Because this addressing automation lets a host learn several key pieces of information in a network, DHCP is sometimes called a *plug-and-play* protocol, whereby hosts can join or leave a network without requiring configuration by network managers.

The convenience of this method of address assignment gives DHCP multiple uses of IP addresses. If any ISP manager does not have a sufficient number of IP addresses, DHCP is used to assign each of its connecting hosts a temporary IP address. When a host joins or leaves, the management server must update its list of available IP addresses. If a host joins the network, the server assigns an available IP address; each time a host leaves, its address is included in the pool of available addresses. DHCP is especially useful in *mobile* IP, with mobile hosts joining and leaving an ISP frequently.

### 7.1.2 Network Address Translation (NAT)

Any IP-type device requires a unique IP address. Because of the growing number of Internet users and devices, each requiring a unique IP address, the issue is critical, especially when a new LAN needs to be added to a community network despite a limited number of IP addresses available for that community. Even in very small residential networks, the issue arises when new devices are added to the network. Although the

numbers of users, servers, or subnets expands over time, the total allocated IP addresses are still limited to a certain level by the associated ISP.

Besides the popularity of IPv6, explained in Chapter 2, an alternative solution, called *network address translation* (NAT), can be used to overcome the challenge presented by this issue.

The idea behind NAT is that all the users and hosts of a private network do not need to have a globally unique addresses. Instead, they can be assigned private and unique addresses within their own private networks, and a NAT-enabled router that connects the private network to the outside world can translate these addresses to globally unique addresses. The NAT-enabled router hides from the outside world the details of the private network. The router acts as a single networking device with a single IP address to the outside world.

For example, assume that a private network with a NAT-enabled router is connecting to the outside world. Suppose that all the machines in this network are internally assigned 128.0.0.0/9 and that the output port of the router is assigned an IP address of 197.36.32.4. Now, this network has the advantage that additional machines or even LANs can be added to it and that each can use an address in the block 128.0.0.0/9. Therefore, users and servers within the network can easily use 128.0.0.0/9 addressing to transmit packets to each other, but packets forwarded beyond the network into the Internet clearly do not use these addresses. This way, thousands of other networks can use the same block of addresses internally. Given a datagram received by the NAT-enabled router, we now need to know how the router knows to which internal host it should deliver the datagram. The answer lies in the use of a *port number* and a *NAT translation table* in the router.

**Example.** Assume that a host with internal address 128.0.0.1 and port number 4527 in a private network requests a connection to a server with IP address 144.55.34.2 and arbitrary port number 3843, which resides in a different country. Suppose that the output port of the connecting NAT router is assigned IP address 197.36.32.4.

***Solution.*** To set up this connection, the host sends its request with source address 128.0.0.1,4527 to the NAT router. The router "translates" this address in its NAT routing table by changing the arbitrary port number from 4527 to an official one of 5557 and changing the internal IP address 128.0.0.1 to its own port IP address, 197.36.32.4. The router then makes the connection request to site 144.55.34.2,3843, using address 197.36.32.4,5557. When the router receives the response from the remote site, the router does the reverse translation and delivers the response to host 128.0.0.1. Although NAT protocol solves the shortage of IP addresses in small communities, it has a

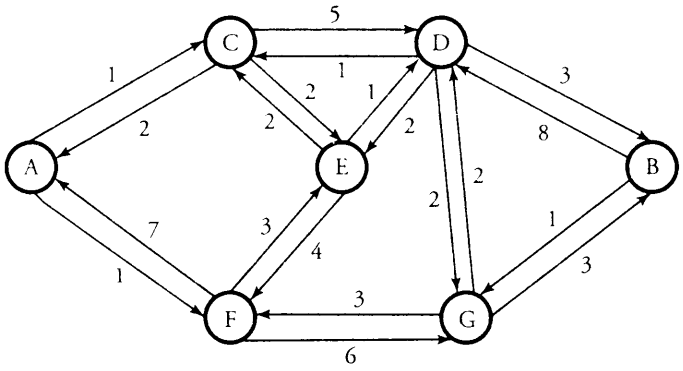


**Figure 7.2** A packet-switched network and all link costs

major drawback of avoiding the assignment of a unique IP address to every networking component.

## 7.1.3 Route Cost

A packet-switched network consists of nodes—routers or switches—that are connected by links. A *link cost* between a pair of source and destination nodes refers to the number of packets currently waiting ahead in the destination node. The goal is to choose a routing based on the *minimum number of hops*, or *least-cost path*. For example, Figure 7.2 shows a network in which the lines between each two nodes represent a link and its cost in its corresponding direction.

The *least-cost path* between each pair of nodes is the minimum cost of the routing between the two nodes, taking into account all possible links between the two nodes. For example, the least-cost path in Figure 7.2 between nodes A and D is not A-C-D. The calculated cost of this path is $1 + 5 = 6$. This is true because the better path is A-C-E-D, with a calculated cost of $1 + 2 + 1 = 4$. Thus, the second case has more paths, but it has a lower cost than the first case, which has a shorter path but a higher cost.

## 7.1.4 Classification of Routing Algorithms

Routing algorithms can be classified in several ways. One way is to classify them as either *least-cost path*, whereby the lowest-cost path must be determined for routing, or *non-least-cost path*, whereby the determination of a route is not based on the cost of a path.

Another way is based on whether an algorithm is *distributed* or *centralized*. In distributed routing, all nodes contribute in making the routing decision for each packet.

In other words, an algorithm in distributed routing allows a node to gain information from all the nodes, but the least-cost path is determined locally. In centralized routing, only a designated node can make a decision. This central node uses the information gained from all nodes, but if the central node fails, the routing function in the network may be interrupted. A special case of centralized routing is *source routing*, whereby the routing decision is made only by the source server rather than by a network node. The outcome is then communicated to other nodes.

Routing can also be classified as either *static* or *dynamic*. In static routing, a network establishes an initial topology of paths. Addresses of initial paths are loaded onto routing tables at each node for a certain period of time. The main disadvantage of static routing is that the size of the network has to be small enough to be controllable. Also, if a failure happens in the network, it is unable to react immediately. In dynamic routing, the state of the network is learned through the communication of each router with its neighbors. Thus, the state of each region in the network is propagated throughout the network after all nodes finally update their routing tables. Each router can find the best path to a destination by receiving updated information from surrounding nodes.

## 7.2 Least-Cost-Path Algorithms

In practice, the majority of Internet routing methods are based on least-cost algorithms. In such algorithms, a link cost is proportional to the links's current traffic load. However, the link cost may not always be proportional to the current load. The link cost is defined on both directions between each pair of nodes. Several least-cost-path algorithms have been developed for packet-switched networks. In particular, *Dijkstra's algorithm* and the *Bellman-Ford algorithm* are the most effective and widely used algorithms.

### 7.2.1 Dijkstra's Algorithm

*Dijkstra's algorithm* is a centralized routing algorithm that maintains information in a central location. The objective is to find the least-cost path from a given source node to all other nodes. This algorithm determines least-cost paths from a source node to a destination node by optimizing the cost in multiple iterations. Dijkstra's algorithm is as follows:

**Begin Dijkstra's Algorithm**

1. **Define:**
   $s$ = Source node
   $k$ = Set of visited nodes by the algorithm

$\alpha_{ij}$ = Cost of the link from node $i$ to node $j$
$\beta_{ij}$ = Cost of the least-cost path from node $i$ to node $j$

2. **Initialize:**
   $K = \{s\}$
   $\beta_{sj} = \alpha_{sj}$ for $j \neq s$
3. **Next node:**
   Find $x \notin k$ that $\beta_{sx} = \min \beta_{sj}$ for $j \notin k$.
   Add $x$ to k.
4. **Least-cost paths:**
   $\beta_{sj} = \min(\beta_{sj}, \beta_{sx} + \alpha_{xj})$ for $j \notin k$ ■

If any two nodes $i$ and $j$ are not connected directly, the cost for that link is infinity, indicated by $\beta_{ij} = \times$. Steps 2 and 3 are repeated until paths are assigned to all nodes. At step 1, $k$ represents $s$, and $\beta_{sj}$ computes the cost of the least-cost path from $s$ to node $j$. At step 2, we want to find $x$ among the neighboring nodes but not in $k$ such that the cost is minimized. At step 3, we simply update the least-cost path. The algorithm ends when all nodes have been visited and included in the algorithm.

**Example.** Using Dijkstra's algorithm, find the least-cost path from node A to node B in Figure 7.2.

***Solution.*** The detailed operation is shown in the Table 7.1. The first step is to find a path from the source node A to all other nodes. Thus, at the fist row, $k$ ={A}. It is obvious that there are direct links from A to nodes C and F. Therefore, the cost of least-cost path for either node is 1, as shown in Figure 7.2. We then fill the table with AC(1) and AF(1), respectively. Given $k$ = {A}, there is no connections between A and nodes D, E, G, and B. The algorithm continues until all nodes have been included as $k$ = A,C,F,E,D,G,B, and we obtain the least-cost path of ACFDB(7).

## 7.2.2 Bellman-Ford Algorithm

The *Bellman-Ford algorithm* finds the least-cost path from a source to a destination by passing through no more than $l$ links. The essence of the algorithm consists of the following steps

**Begin Bellman-Ford Algorithm**

1. **Define:**
   $s$ = Source node
   $\alpha_{ij}$ = Cost of the link from node $i$ to node $j$
   $\beta_{ij}(l)$ = Cost of the least-cost path from $i$ to $j$ with no more than $l$ links