CBCS SCHEME

USN | | | | | | | | | | |

18CS46

Fourth Semester B.E. Degree Examination, July/August 2022
Data Communication

Time: 3 hrs. Max. Marks: 100

Note: Answer any FIVE full questions, choosing ONE full question from each module.

Module-1

1 a. What is Data Communication? With neat diagram, explain the components of data communication. **(08 Marks)**

b. With neat diagram, explain four basic topologies. Assume that 10 devices are connected in mesh topology. How many duplex links are needed? How many ports are needed for each device? **(08 Marks)**

c. Explain Half Duplex and Full Duplex with respect to data communication. **(04 Marks)**

OR

2 a. With neat diagram, explain TCP/IP protocol suite of computer networks. **(08 Marks)**

b. Define transmission impairments. Explain different, causes of transmission impairment during signal transmission. **(08 Marks)**

c. Explain briefly about Shannon capacity and Nyquist bit rate for communication channel. **(04 Marks)**

Module-2

3 a. With neat diagram, explain the most common technique to change analog signal to digital signal. **(12 Marks)**

b. With a neat diagram, explain ASK, FSK and PSK. **(06 Marks)**

c. In a digital transmission the receiver clock is 0.3 percent faster than the sender clock. How many extra bits per second does the receiver receive if the data rate is 1 Mbps? **(02 Marks)**

OR

4 a. Define line coding. List out its characteristics. Represent the sequence "01001110" using NRZ-L, NRZ-I and Manchester scheme. **(10 Marks)**

b. Explain parallel and serial transmission modes. **(06 Marks)**

c. An analog signal has a bit rate of 8000 bps and baud rate of 1000 baud. How many data elements are carried by each signal element? How many signal elements do we need? **(04 Marks)**

Module-3

5 a. What is circuit switching? Enumerate the characteristics of circuit switching. Analyze the three stages of circuit switching. **(10 Marks)**

b. What is multiplexing? Explain wavelength division multiplexing. **(05 Marks)**

c. Given data word 101001111 and devisor 10111. Show the generation of CRC codeword at the sender site. **(05 Marks)**

OR

6 a. What is spread spectrum? Explain FHSS and DHSS. **(10 Marks)**

b. Analyze how message can be transferred from one system to another using datagram network and calculate the delay in the network. **(05 Marks)**

c. Assume a packet is made any of four 16 bits words $(466F)_{16}$, $(726F)_{16}$, $(757A)_{16}$ and $(616E)_{16}$. Find the sender site checksum using traditional checksum algorithm. **(05 Marks)**

Module-4

7 a. With neat diagram, explain point-to-point protocol frame format. **(06 Marks)**
b. Explain pure ALOHA and slotted ALOHA protocols. **(08 Marks)**
c. Explain the working of stop-and-wait protocol for Noiseless channels. **(06 Marks)**

OR

8 a. Analyze channelization. Explain Code Division Multiple Access (CDMA). **(08 Marks)**
b. Mention different controlled access methods. Explain token passing method. **(06 Marks)**
c. Explain class full addressing of IPV4. **(06 Marks)**

Module-5

9 a. Explain the operation of Cellular Telephony. **(08 Marks)**
b. Explain Bluetooth Architecture. **(05 Marks)**
c. Explain the different types of addressing mechanisms in IEEE-802.11. **(07 Marks)**

OR

10 a. With neat diagram, explain Ethernet frame format. **(10 Marks)**
b. Explain access control of wireless LAN. **(05 Marks)**
c. Explain Fourth Generation (4G) of Cellular Telephone. **(05 Marks)**

* * * * *

1a) Data communication is the exchange of data between two or more devices through some form of transmission medium. Data can be in any format like text, image, number, audio, and video.

A data communications system has five components as shown in the below figure.

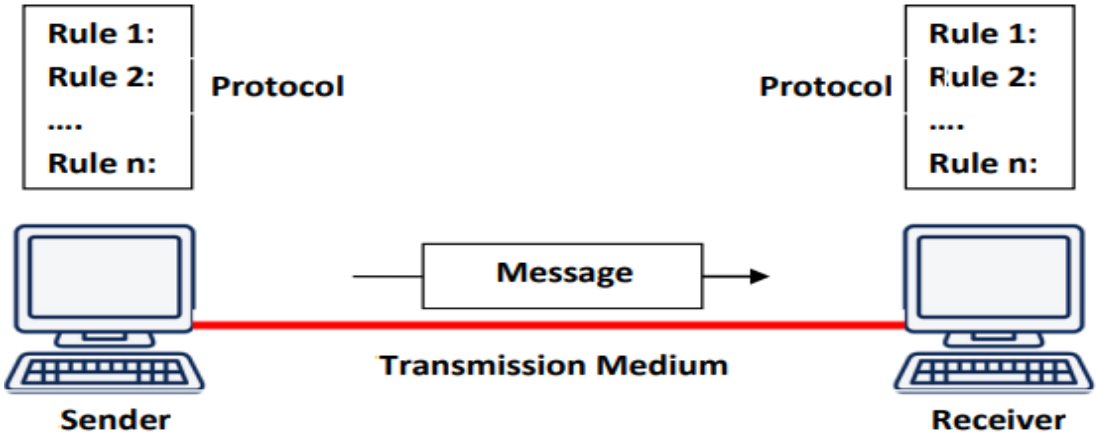
1.Message: The message is the data to be transmitted. Data can be text, numbers, pictures, audio, and video.

2. Sender: The sender is the device that sends the data. It can be a computer, workstation, telephone handset, video camera, and so on.

3. Receiver: The receiver is the device that receives the data. It can be a computer, workstation, telephone handset, television, and so on.

4. Transmission medium: The transmission medium is the physical path by which a message travels from sender to receiver. It can be wired or wireless medium.

5. Protocol: A protocol is a set of rules that govern data communications. It represents an agreement between the communicating devices.

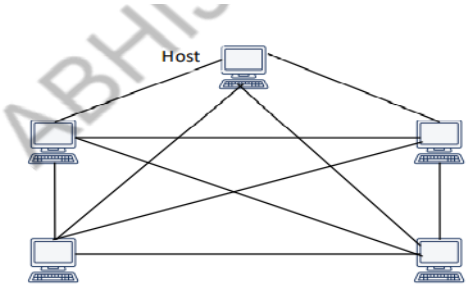


1b) There are four basic topologies: mesh, star, bus, and ring.

1) Mesh Topology

In a mesh topology, every device has a dedicated point-to-point link to every other device.

To accommodate many links, every device on the network must have n – 1 input/output (I/O) ports to be connected to the other n - 1 stations.



Advantages

The use of dedicated links guarantees that each connection can carry its own data load, thus eliminating the traffic problems that can occur when links are shared between multiple devices.

A mesh topology is robust. If one link becomes unusable, it does not affect the entire system.

There is the advantage of privacy or security. When every message travels along a dedicated line, only the intended recipient sees it. Physical boundaries prevent other users from gaining access to messages.

Point-to-point links make fault identification and fault isolation easy.

Disadvantages

• The amount of cabling and the number of I/O ports required is more because every device must be connected to every other device, installation and reconnection are difficult.

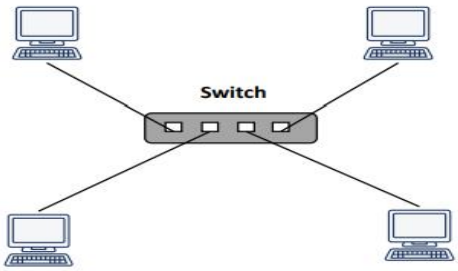
• The sheer bulk of the wiring can be greater than the available space (in walls, ceilings, or floors) can accommodate.

• The hardware required to connect each link (I/O ports and cable) is expensive.

2) Star Topology

In a star topology, each device has a dedicated point-to-point link only to a central controller, called as switch.

The devices are not directly connected to one another. If one device wants to send data to another , it sends the data to the switch, which then relays the data to the other connected device.



Advantages: • A star topology is less expensive than a mesh topology.

• In a star, each device needs only one link and one I/O port to connect it to any number of others. This factor also makes it easy to install and reconfigure.

• The robustness. If one link fails, only that link is affected. All other links remain active.

• Fault isolation and identification is easy.

• As long as the hub is working, it can be used to monitor link problems and bypass defective links.

Disadvantages:

• One big disadvantage of a star topology is the dependency of the whole topology on one single point, the hub. If the hub goes down, the whole system is dead.

3) Bus Topology

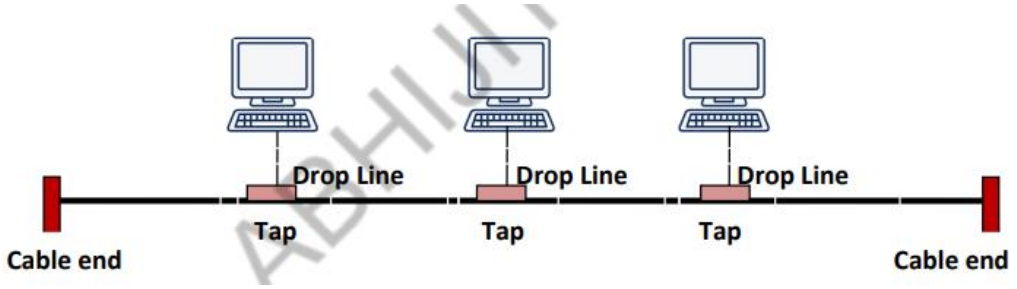
A bus topology is multipoint. All the devices in a network are connected through a single link, which acts as a backbone.

Nodes are connected to the bus cable by drop lines and taps.

A drop line is a connection running between the device and the main cable.

A tap is a connector that either splices into the main cable or punctures the sheathing of a cable to create a contact with the metallic core.

As a signal travels along the backbone, some of its energy is transformed into heat. Therefore, it becomes weaker and weaker as it travels farther and farther.



Advantages:

• Ease of Installation.

• A bus uses less cabling than mesh or star topologies.

Disadvantage:

• Difficult reconnection and fault isolation.

• A bus is usually designed to be optimally efficient at installation. It can therefore be difficult to add new devices.

• Signal reflection at the taps can cause degradation in quality.

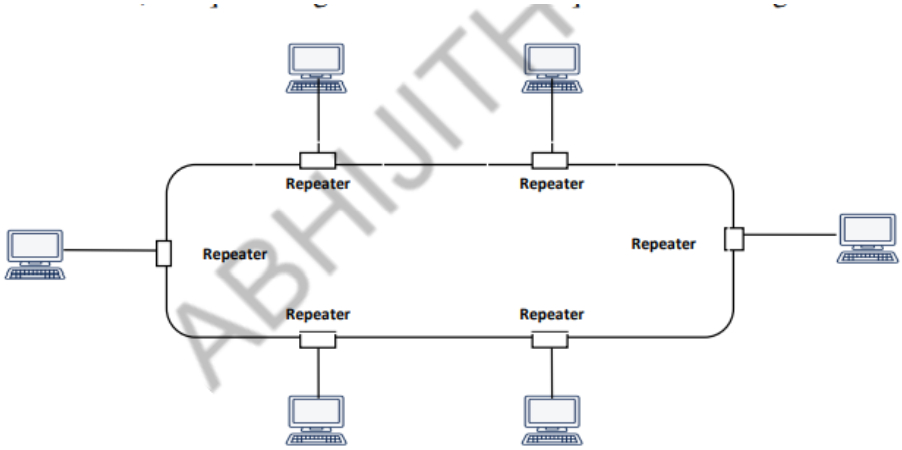
• A fault or break in the bus cable stops all transmission, even between devices on the same side of the problem

4) Ring Topology

• In a ring topology, each device has a dedicated point-to-point connection with only the two devices on either side of it.

• A signal is passed along the ring in one direction until it reaches its destination.

• Each device in the ring uses a repeater. When a device receives a signal intended for another device, its repeater regenerates the bits and passes them along



Advantages:

• A ring is relatively easy to install and reconfigure.

• Each device is linked to only its immediate neighbours. Hence adding or deleting a device requires changing only two connections.

• Fault Isolation is simplified.

Disadvantages:

• Unidirectional traffic.

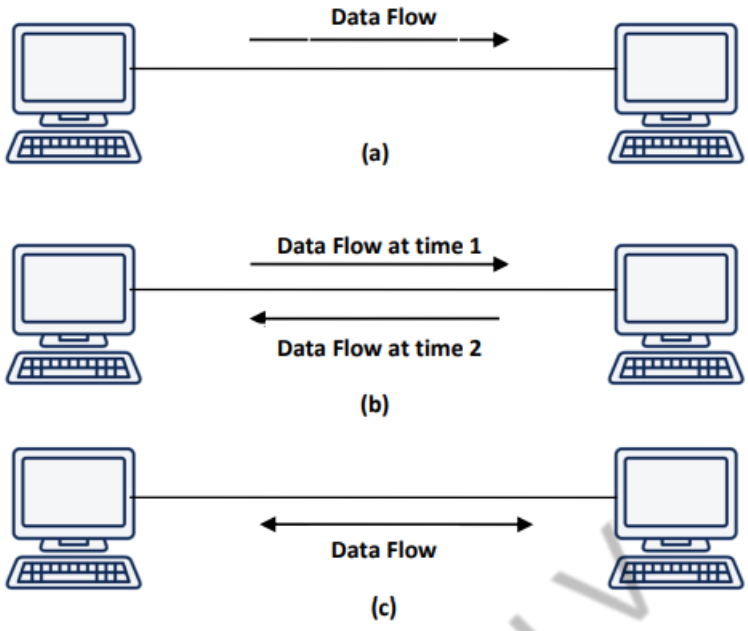
• In a simple ring, a break in the ring can disable the entire network.

1c) Data Flow Communication between two devices can be simplex, half-duplex, or full-duplex.

• Simplex: In simplex mode, the communication is unidirectional. Only one of the two devices on a link can transmit; the other can only receive. Example: Keyboards and traditional monitors.

• Half-Duplex: In half-duplex mode, each station can both transmit and receive, but not at the same time. When one device is sending, the other can only receive, and vice versa. The entire capacity of the channel can be utilized for each direction. Example: Walkie-talkies.

• Full-Duplex: In full-duplex mode (also called duplex), both stations can transmit and receive simultaneously. The capacity of the channel is divided between the two directions. Example: telephone network.

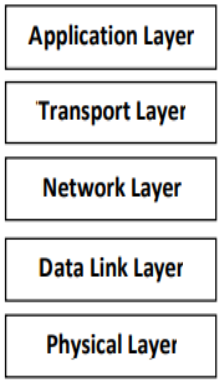


(a) Simplex mode (b) Half Duplex mode (c) Full Duplex mode of communication

2a) TCP/IP Protocol Suite

• TCP/IP is a protocol suite (a set of protocols organized in different layers) used in the Internet today.

• It is a hierarchical protocol made up of interactive modules, each of which provides a specific functionality. The term hierarchical means that each upper level protocol is supported by the services provided by one or more lower level protocols.



2.2.1 Layered Architecture

• Each device is involved with a set of layers depending on the role of the device in the internet. The two hosts (source and destination) are involved in all five layers.

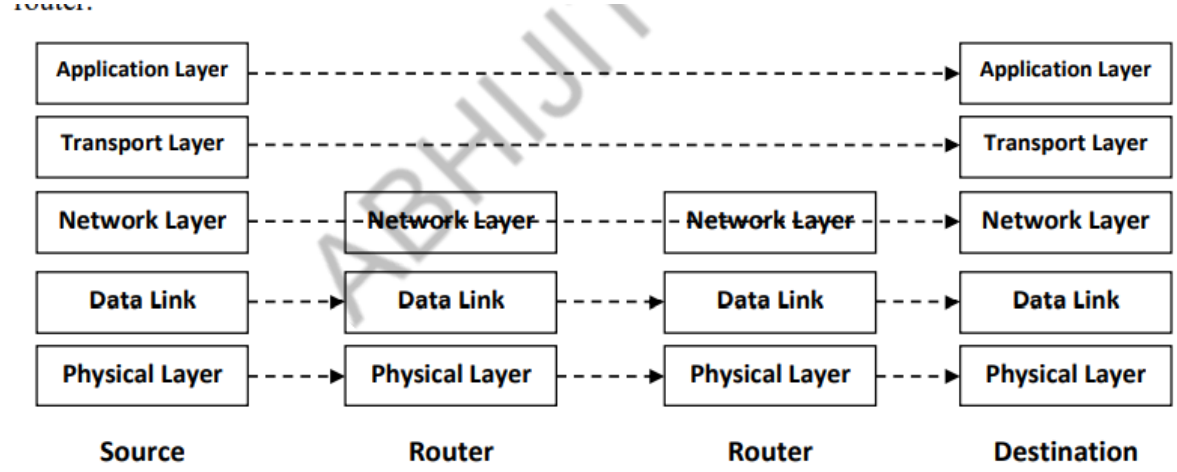
• The source creates message in the application layer and send it down the layers so that it is physically sent to the destination. The destination host needs to receive the communication at the physical layer and then deliver it through the other layers to the application layer.

• The router is involved in only three layers: Network layer, Data Link layer, physical layer. There is no transport or application layer in a router as long as the router is used only for routing.

• A link-layer switch in a link, however, is involved only in two layers, data-link and physical.

Layers in the TCP/IP Protocol Suite

As the figure shows, the duty of the application, transport, and network layers is end-to-end. However, the duty of the data-link and physical layers is hop-to-hop, in which a hop is a host or router.



Description of Each Layer

1) Physical Layer

• Physical layer is responsible for carrying individual bits in a frame across the link.

• The communication between two devices at the physical layer is still a logical communication because there transmission media under the physical layer. Two devices are connected by a transmission medium (cable or air).

• The transmission medium does not carry bits; it carries electrical or optical signals. So the bits received in a frame from the data-link layer are transformed and sent through the transmission media.

2) Data-link Layer

• There may be several overlapping sets of links that a datagram can travel from the host to the destination. The routers are responsible for choosing the best links.

• The link can be a wired LAN with a link-layer switch, a wireless LAN, a wired WAN, or a wireless WAN. We can also have different protocols used with any link type. In each case, the data-link layer is responsible for moving the packet through the link.

• TCP/IP does not define any specific protocol for the data-link layer. It supports all the standard and proprietary protocols. Any protocol that can take the datagram and carry it through the link suffices for the network layer. The data-link layer takes a datagram and encapsulates it in a packet called a frame.

• Each link-layer protocol may provide a different service. Some link-layer protocols provide complete error detection and correction, some provide only error correction.

3) Network Layer

• The network layer is responsible for creating a connection between the source and destination.

• The network layer is responsible for host-to-host communication and routing the packet through possible routes.

• The network layer in the Internet includes the main protocol, Internet Protocol (IP), that defines the format of the packet, called a datagram at the network layer. IP also defines the format and the structure of addresses used in this layer.

• IP is also responsible for routing a packet from its source to its destination.

• IP is a connectionless protocol that provides no flow control, no error control, and no congestion control services. If any of these services is required for an application, the application should rely only on the transport-layer protocol.

• The network layer also has some auxiliary protocols that help IP in its delivery and routing tasks.

▪ The Internet Control Message Protocol (ICMP) helps IP to report some problems when routing a packet.

▪ The Internet Group Management Protocol (IGMP) is another protocol that helps IP in multitasking.

▪ The Dynamic Host Configuration Protocol (DHCP) helps IP to get the network-layer address for a host.

▪ The Address Resolution Protocol (ARP) is a protocol that helps IP to find the link-layer address of a host or a router when its network-layer address is given.

4) Transport Layer

• The transport layer at the source host gets the message from the application layer, encapsulates it in a transport layer packet called a segment and sends it, through the logical connection, to the transport layer at the destination host.

• The transport layer is responsible for giving services to the application layer: to get a message from an application program running on the source host and deliver it to the corresponding application program on the destination host. There are a few transport-layer protocols in the Internet, each designed for some specific task.

5) Application Layer

• The application layer enables the user to access the network.

• Communication at the application layer is between two processes. To communicate, a process sends a request to the other process and receives a response. Process-to-process communication is the duty of the application layer.

• It provides user interfaces and support for services such as electronic mail, remote file access and transfer, shared database management, and other types of distributed information services.

2b) Transmission Impairment

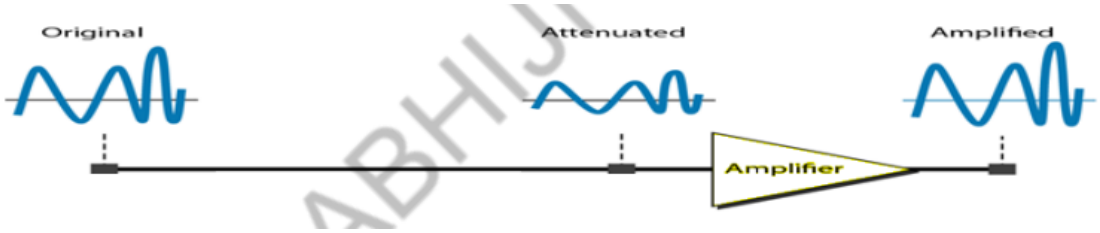
Signals travel through transmission media, which are not perfect. The imperfection causes signal impairment. Three causes of impairment are attenuation, distortion, and noise.

Attenuation

• Attenuation means a loss of energy.

• When a signal, simple or composite, travels through a medium, it loses some of its energy in overcoming the resistance of the medium.

• To compensate for this loss, amplifiers are used to amplify the signal.



Decibel: The decibel (dB) measures the relative strengths of two signals or one signal at two different points. The decibel is negative if a signal is attenuated and positive if a signal is amplified. dB = 10log10 (P2/P1) Variables PI and P2 are the powers of a signal at points 1 and 2, respectively.

Distortion

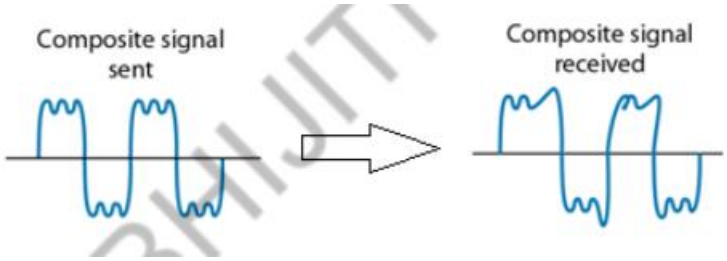
• Distortion means that the signal changes its form or shape.

• Distortion can occur in a composite signal made of different frequencies.

• Each signal component has its own propagation speed (see the next section) through a medium and, therefore, its own delay in arriving at the final destination.

• Differences in delay may create a difference in phase if the delay is not exactly the same as the period duration.

• In other words, signal components at the receiver have phases different from what they had at the sender. The shape of the composite signal is therefore not the same.



Noise

• Noise is another cause of impairment.

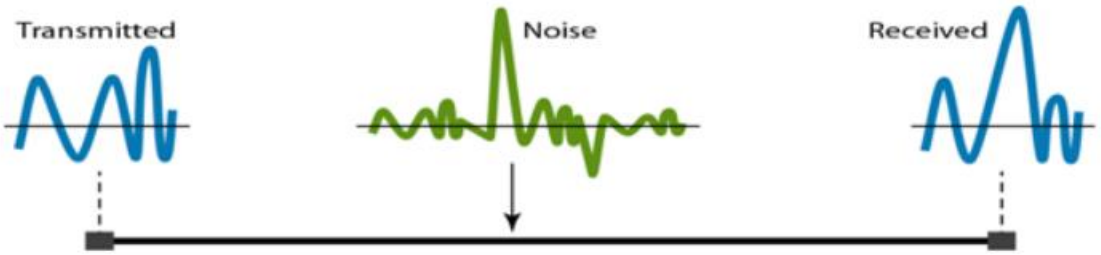
• Several types of noise, such as thermal noise, induced noise, crosstalk, and impulse noise, may corrupt the signal.

• Thermal noise is the random motion of electrons in a wire which creates an extra signal not originally sent by the transmitter.

• Induced noise comes from sources such as motors and appliances. These devices act as a sending antenna, and the transmission medium acts as the receiving antenna.

• Crosstalk is the effect of one wire on the other. One wire acts as a sending antenna and the other as the receiving antenna.

• Impulse noise is a spike (a signal with high energy in a very short time) that comes from power lines, lightning, and so on.



2c)

Noisy Channel: Shannon Capacity

In reality, we cannot have a noiseless channel; the channel is always noisy. In 1944, Claude Shannon introduced a formula, called the Shannon capacity, to determine the theoretical highest data rate for a noisy channel:

Capacity =bandwidth X log2 (1 +SNR)

In this formula, bandwidth is the bandwidth of the channel, SNR is the signal-to noise ratio, and capacity is the capacity of the channel in bits per second.

Noiseless Channel: Nyquist Bit Rate

For a noiseless channel, the Nyquist bit rate formula defines the theoretical maximum bit rate

BitRate = 2 x bandwidth x log2 L

In this formula, bandwidth is the bandwidth of the channel, L is the number of signal levels used to represent data, and Bit Rate is the bit rate in bits per second. Increasing the levels of a signal may reduce the reliability of the system.

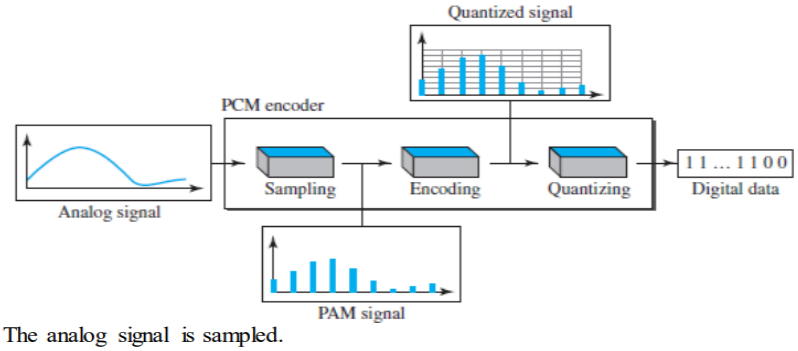
3a) ANALOG-TO-DIGITAL CONVERSION

Sometimes, we have an analog signal such as one created by a microphone or camera. The tendency today is to change an analog signal to digital data.

Two techniques - pulse code modulation and delta modulation are used for this conversion of analog signal into digital data. After the digital data are created (digitization), we can use one of the techniques described in the previous module to convert the digital data to a digital signal.

Pulse Code Modulation (PCM)

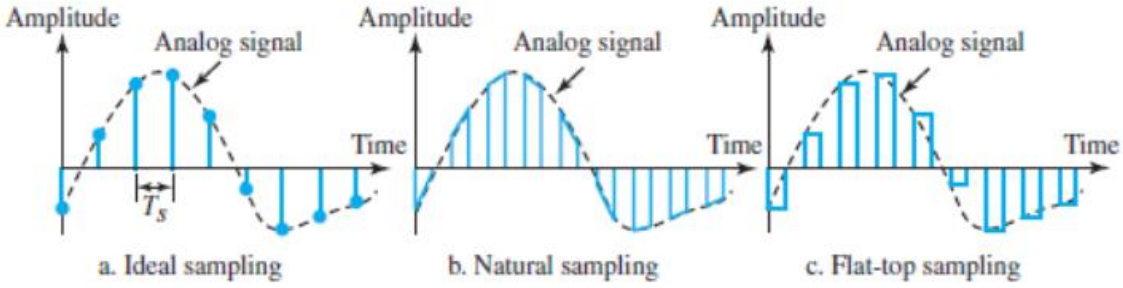
The most common technique to change an analog signal to digital data (digitization) is called pulse code modulation (PCM). A PCM encoder has three processes, as shown in the below figure.



1. The analog signal is sampled.
2. The sampled signal is quantized.
3. The quantized values are encoded as streams of bits.

i. Sampling

The first step in PCM is sampling. The analog signal is sampled every Ts s, where Ts is the sample interval or period. The inverse of the sampling interval is called the sampling rate or sampling frequency and denoted by fs, where fs = 1/Ts. There are three sampling methods— ideal, natural, and flat-top as shown in the next figure.



In ideal sampling, pulses from the analog signal are sampled. This is an ideal sampling method and cannot be easily implemented. In natural sampling, a high-speed switch is turned on for only the small period of time when the sampling occurs. The result is a sequence of samples that retains the shape of the analog signal. The most common sampling method, called sample and hold, however, creates flat-top samples by using a circuit. The sampling process is sometimes referred to as pulse amplitude modulation (PAM). The result of sampling is still an analog signal with nonintegral values.

ii. Quantization

The result of sampling is a series of pulses with amplitude values between the maximum and minimum amplitudes of the signal. The set of amplitudes can be infinite with nonintegral values between the two limits. These values cannot be used in the encoding process. The following are the steps in quantization:

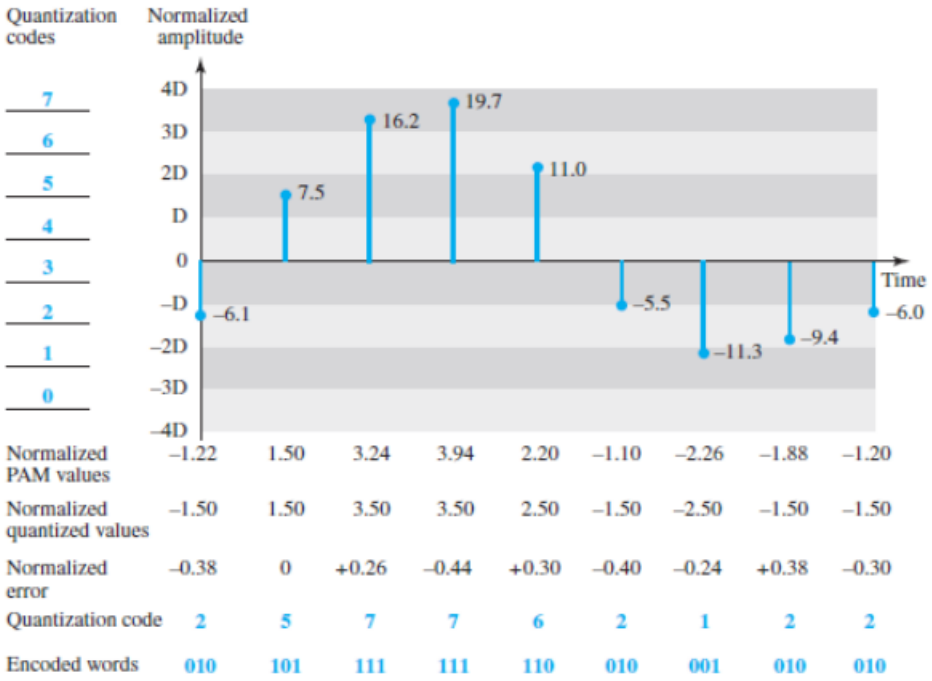
a. We assume that the original analog signal has instantaneous amplitudes between Vmin and Vmax.

b. We divide the range into L zones, each of height Δ (delta).

c. We assign quantized values of 0 to L − 1 to the midpoint of each zone.

d. We approximate the value of the sample amplitude to the quantized values.

For example, assume that we have a sampled signal and the sample amplitudes are between −20 and +20 V. We decide to have eight levels (L = 8). This means that Δ = 5 V. Figure shows this example.



Normalized PAM values	–1.22	1.50	3.24	3.94	2.20	–1.10	–2.26	–1.88	–1.20
Normalized quantized values	–1.50	1.50	3.50	3.50	2.50	–1.50	–2.50	–1.50	–1.50
Normalized error	–0.38	0	+0.26	–0.44	+0.30	–0.40	–0.24	+0.38	–0.30
Quantization code	2	5	7	7	6	2	1	2	2
Encoded words	010	101	111	111	110	010	001	010	010

We have shown only nine samples using ideal sampling (for simplicity). The value at the top of each sample in the graph shows the actual amplitude. In the chart, the first row is the normalized value for each sample (actual amplitude/Δ). The quantization process selects the quantization value from the middle of each zone. This means that the normalized quantized values (second row) are different from the normalized amplitudes. The difference is called the normalized error (third row). The fourth row is the quantization code for each sample based on the quantization levels at the left of the graph. The encoded words (fifth row) are the final products of the conversion.

Quantization Levels

In the previous example, we showed eight quantization levels. The choice of L, the number of levels, depends on the range of the amplitudes of the analog signal and how accurately we need to recover the signal. If the amplitude of a signal fluctuates between two values only, we need

only two levels; if the signal, like voice, has many amplitude values, we need more quantization levels. In audio digitizing, L is normally chosen to be 256; in video it is normally thousands. Choosing lower values of L increases the quantization error if there is a lot of fluctuation in the signal.

Quantization Error

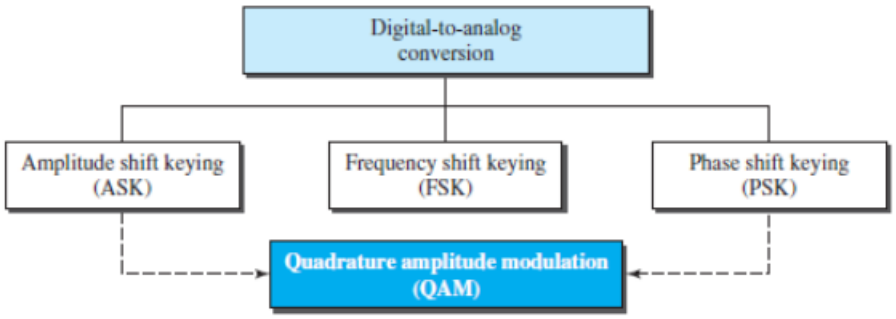
One important issue is the error created in the quantization process. Quantization is an approximation process. The input values to the quantizer are the real values; the output values are the approximated values. The output values are chosen to be the middle value in the zone. If the input value is also at the middle of the zone, there is no quantization error; otherwise, there is an error. In the previous example, the normalized amplitude of the third sample is 3.24, but the normalized quantized value is 3.50. This means that there is an error of +0.26. The value of the error for any sample is less than Δ/2. In other words, we have $-\Delta/2 \leq \text{error} \leq \Delta/2$.

iii. Encoding

The last step in PCM is encoding. After each sample is quantized and the number of bits per sample is decided, each sample can be changed to an nb-bit code word. In the previous figure, the encoded words are shown in the last row. A quantization code of 2 is encoded as 010; 5 is encoded as 101; and so on. Note that the number of bits for each sample is determined from the number of quantization levels. If the number of quantization levels is L, the number of bits is nb = log2 L. In our example L is 8 and nb is therefore 3. The bit rate can be found from the formula

$$\text{Bit rate} = \text{sampling rate} \times \text{number of bits per sample} = f_s \times n_b$$

3b) Digital-to-analog conversion is the process of changing one of the characteristics of an analog signal based on the information in digital data.



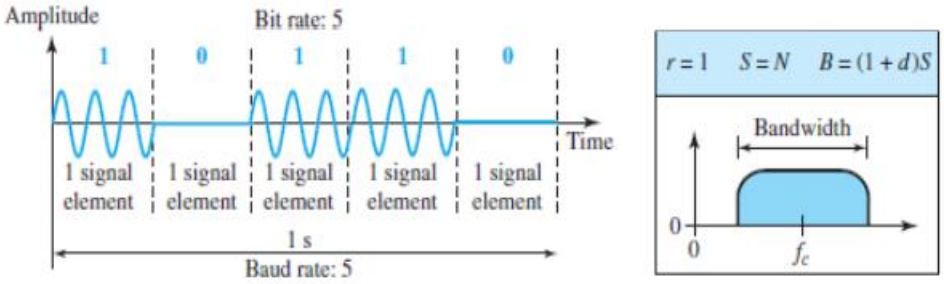
Amplitude Shift Keying

In amplitude shift keying, the amplitude of the carrier signal is varied to create signal elements. Both frequency and phase remain constant while the amplitude changes.

1. Binary ASK

(BASK) ASK is normally implemented using only two levels. This is referred to as binary amplitude shift keying or on- off keying (OOK). The peak amplitude of one signal level is 0; the

other is the same as the amplitude of the carrier frequency. Figure 5.3 gives a conceptual view of binary ASK.



Bandwidth for ASK The above figure also shows the bandwidth for ASK. Although the carrier signal is only one simple sine wave, the process of modulation produces a nonperiodic composite signal.

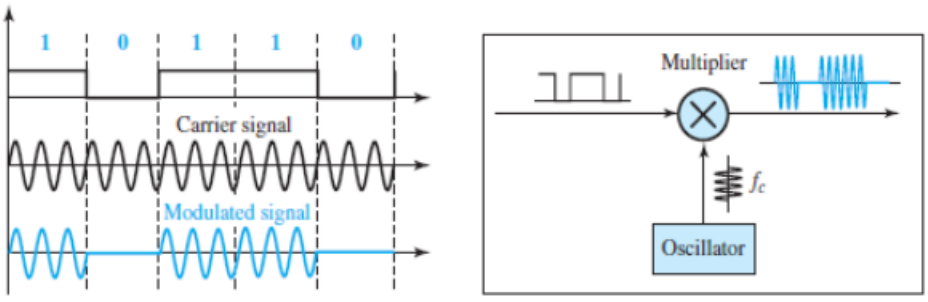
As we expect, the bandwidth is proportional to the signal rate (baud rate). However, there is normally another factor involved, called d, which depends on the modulation and filtering process.

The value of d is between 0 and 1. This means that the bandwidth can be expressed as shown, where 5 is the signal rate and the B is the bandwidth. B = (1 +d) x S The formula shows that the required bandwidth has a minimum value of S and a maximum value of 2S.

The most important point here is the location of the bandwidth. The middle of the bandwidth is where fc, the carrier frequency, is located.

This means if we have a bandpass channel available, we can choose our fc so that the modulated signal occupies that bandwidth.

This is in fact the most important advantage of digital to- analog conversion. We can shift the resulting bandwidth to match what is available. The next figure shows how we can simply implement binary ASK.



If digital data are presented as a unipolar NRZ digital signal with a high voltage of I V and a low voltage of 0 V, the implementation can achieved by multiplying the NRZ digital signal by the carrier signal coming from an oscillator. When the amplitude of the NRZ signal is 1, the amplitude of the carrier frequency is held; when the amplitude of the NRZ signal is 0, the amplitude of the carrier frequency is zero.

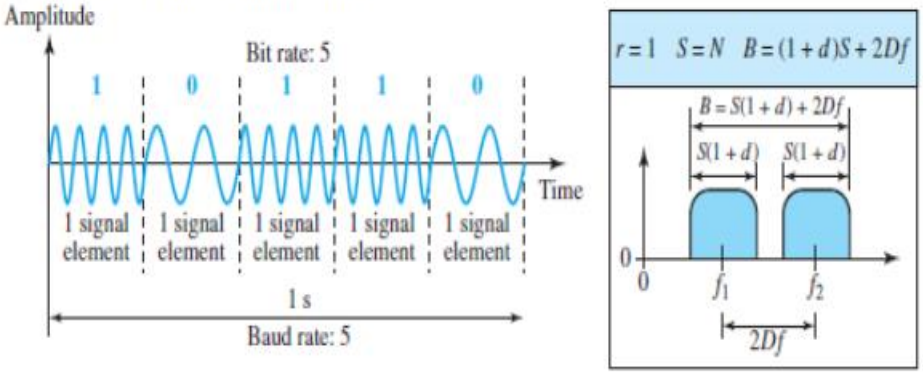
Multilevel ASK

The above discussion uses only two amplitude levels. We can have multilevel ASK in which there are more than two levels. We can use 4,8, 16, or more different amplitudes for the signal and modulate the data using 2, 3, 4, or more bits at a time. In these cases, r = 2, r = 3, r =4, and so on. Although this is not implemented with pure ASK, it is implemented with QAM (as we will see later).

Frequency Shift Keying

In frequency shift keying, the frequency of the carrier signal is varied to represent data. The frequency of the modulated signal is constant for the duration of one signal element, but changes for the next signal element if the data element changes. Both peak amplitude and phase remain constant for all signal elements Binary FSK (BFSK) One way to think about binary FSK (or BFSK) is to consider two carrier frequencies. In Figure 5.6, we have selected two carrier frequencies,f1 and f2. We use the first carrier if the data element is 0; we use the second if the data element is 1.

Figure 5.6 *Binary frequency shift keying*



As Figure 5.6 shows, the middle of one bandwidth is f1 and the middle of the other is f2. Both f1 and f2 are Δf apart from the midpoint between the two bands.

The difference between the two frequencies is 2Δf. Bandwidth for BFSK Figure 5.6 also shows the bandwidth of FSK. Again the carrier signals are only simple sine waves, but the modulation creates a nonperiodic composite signal with continuous frequencies. We can think of FSK as two ASK signals, each with its own carrier frequency f1 and f2). If the difference between the two frequencies is 2Δf, then the required bandwidth is B = (l+d) x S+2Δf.

Implementation

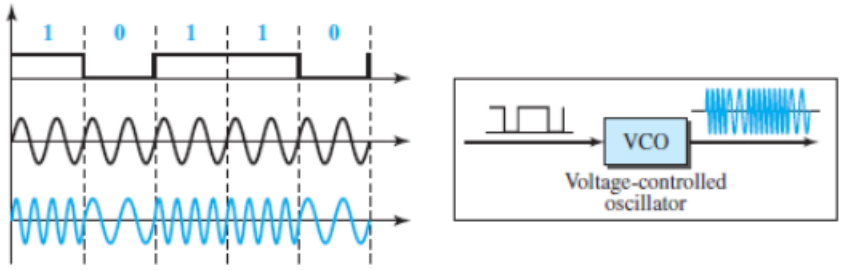
There are two implementations of BFSK: noncoherent and coherent.

In noncoherent BFSK, there may be discontinuity in the phase when one signal element ends and the next begins.

In coherent BFSK, the phase continues through the boundary of two signal elements.

Noncoherent BFSK can be implemented by treating BFSK as two ASK modulations and using two carrier frequencies. Coherent BFSK can be implemented by using one voltage controlled oscillator (VeO) that changes its frequency according to the input voltage.

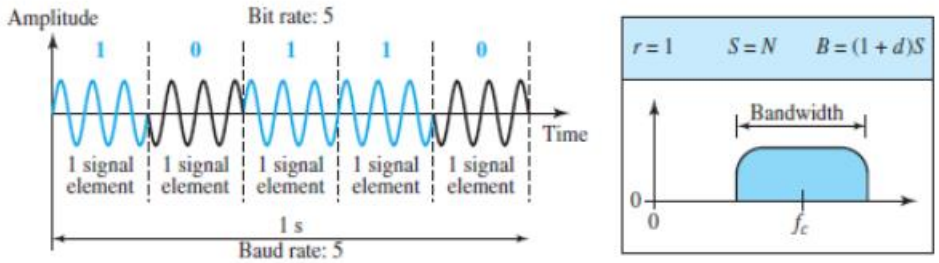
The input to the oscillator is the unipolar NRZ signal. When the amplitude of NRZ is zero, the oscillator keeps its regular frequency; when the amplitude is positive, the frequency is increased.



Multilevel FSK Multilevel modulation (MFSK) is not uncommon with the FSK method. We can use more than two frequencies. For example, we can use four different frequencies f1,f2,f3, and f4 to send 2 bits at a time. To send 3 bits at a time, we can use eight frequencies. However, we need to remember that the frequencies need to be 2Δf apart. For the proper operation of the modulator and demodulator, it can be shown that the minimum value of 2Δf needs to be S. We can show that the bandwidth with d =0 is B= (l +d) x S + (L - 1) 2Δf ◊ B =Lx S.

Phase Shift Keying

In phase shift keying, the phase of the carrier is varied to represent .two or more different signal elements. Both peak amplitude and frequency remain constant as the phase changes. Today, PSK is more common than ASK or FSK. QAM, which combines ASK and PSK, is the dominant method of digital-to- analog modulation. Binary PSK (BPSK) The simplest PSK is binary PSK, in which we have only two signal elements, one with a phase of 0°, and the other with a phase of 180°. Figure 5.9 gives a conceptual view of PSK. Binary PSK is as simple as binary ASK with one big advantage-it is less susceptible to noise.



In ASK, the criterion for bit detection is the amplitude of the signal; in PSK, it is the phase. Noise can change the amplitude easier than it can change the phase. In other words, PSK is less susceptible to noise than ASK.PSK is superior to FSK because we do not need two carrier signals.

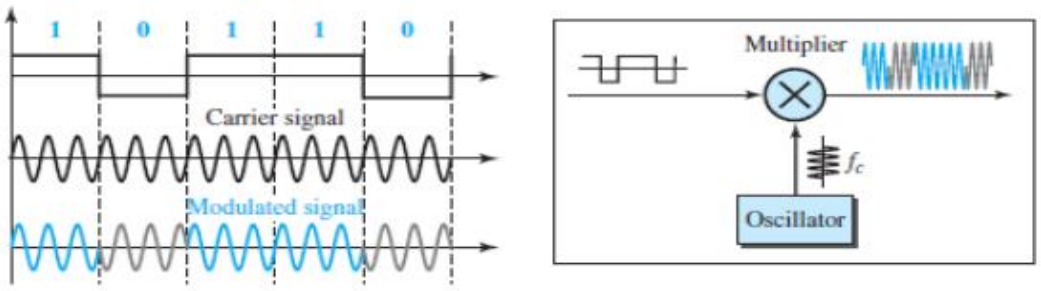
Bandwidth

Figure 5.9 also shows the bandwidth for BPSK. The bandwidth is the same as that for binary ASK, but less than that for BFSK. No bandwidth is wasted for separating two carrier signals.

Implementation

The implementation of BPSK is as simple as that for ASK. The reason is that the signal element with phase 180° can be seen as the complement of the signal element with phase 0°. This gives us a clue on how to implement BPSK. We use the same idea we used for ASK but with a polar NRZ signal instead of a unipolar NRZ signal, as shown in Figure 5.10. The polar NRZ signal is

multiplied by the carrier frequency; the 1 bit (positive voltage) is represented by a phase starting at 0°; the 0 bit (negative voltage) is represented by a phase starting at 180°.



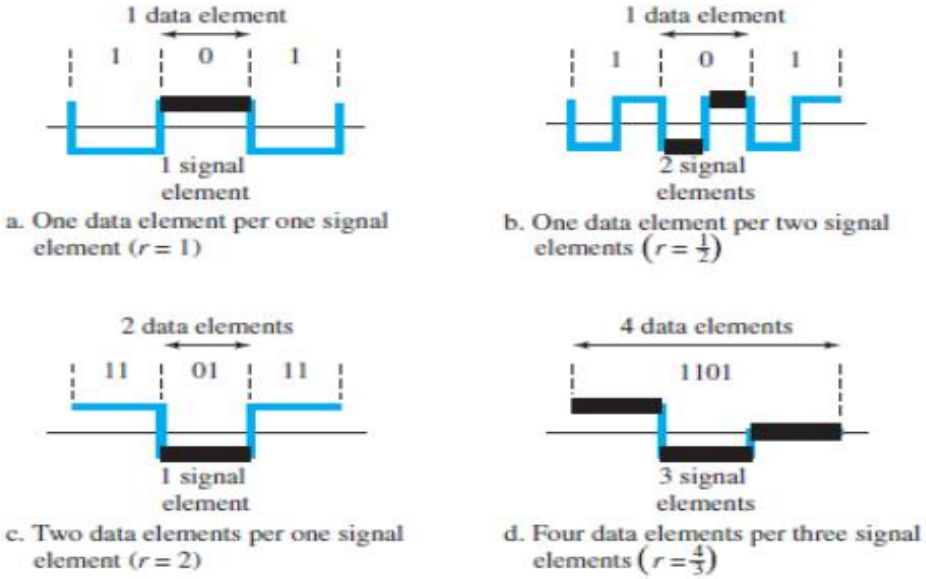
4a)

4.1.1 Line Coding

• Line coding is the process of converting digital data to digital signals.

Characteristics of line coding

1. Signal Element Versus Data Element • A data element is the smallest entity that can represent a piece of information: this is the bit. In digital data communications, a signal element carries data elements. • A signal element is the shortest unit (timewise) of a digital signal. • In other words, data elements are what we need to send; signal elements are what we can send. Data elements are being carried; signal elements are the carriers. We define a ratio r which is the number of data elements carried by each signal element. Figure 4.2 shows several situations with different values of r.



In part a of the figure, one data element is carried by one signal element (r = 1). In part b of the figure, we need two signal elements (two transitions) to carry each data element (r =). We will see later that the extra signal element is needed to guarantee synchronization. In part c of the

figure, a signal element carries two data elements (r = 2). Finally, in part d, a group of 4 bits is being carried by a group of three signal elements (r = 4/3).

2. Data Rate Versus Signal Rate The data rate defines the number of data elements (bits) sent in 1s. The unit is bits per second (bps). The signal rate is the number of signal elements sent in 1s. The unit is the baud. The data rate is sometimes called the bit rate; the signal rate is sometimes called the pulse rate, the modulation rate, or the baud rate. One goal in data communications is to increase the data rate while decreasing the signal rate. Increasing the data rate increases the speed of transmission; decreasing the signal rate decreases the bandwidth requirement. Consider the relationship between data rate (N) and signal rate (S).

$$S = N/r$$

in which r has been previously defined. This relationship, of course, depends on the value of r. It also depends on the data pattern. If we have a data pattern of all 1s or all 0s, the signal rate may be different from a data pattern of alternating 0s and 1s. To derive a formula for the relationship, we need to define three cases: the worst, best, and average. The worst case is when we need the maximum signal rate; the best case is when we need the minimum. In data communications, we are usually interested in the average case. We can formulate the relationship between data rate and signal rate as

$$S_{ave} = c \times N \times (1/r) \quad \text{baud}$$

where N is the data rate (bps); c is the case factor, which varies for each case; S is the number of signal elements per second; and r is the previously defined factor.

3. Bandwidth A digital signal that carries information is nonperiodic. The bandwidth of a nonperiodic signal is continuous with an infinite range. However, most digital signals we encounter in real life have a bandwidth with finite values. In other words, the bandwidth is theoretically infinite, but many of the components have such a small amplitude that they can be ignored. The effective bandwidth is finite. The baud rate determines the required bandwidth for a digital signal. The bandwidth reflects the range of frequencies we need. There is a relationship between the baud rate (signal rate) and the bandwidth. The bandwidth (range of frequencies) is proportional to the signal rate (baud rate). The minimum bandwidth can be given as

$$B_{min} = c \times N \times (1/r)$$

We can solve for the maximum data rate if the bandwidth of the channel is given.

$$N_{max} = (1/c) \times B \times r$$

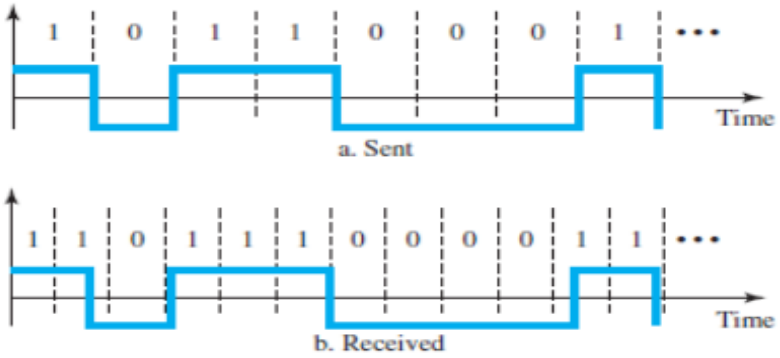
4. Baseline Wandering

In decoding a digital signal, the receiver calculates a running average of the received signal power. This average is called the baseline. The incoming signal power is evaluated against this baseline to determine the value of the data element. A long string of 0s or 1s can cause a drift in the baseline (baseline wandering) and make it difficult for the receiver to decode correctly. A good line coding scheme needs to prevent baseline wandering.

5. DC Components

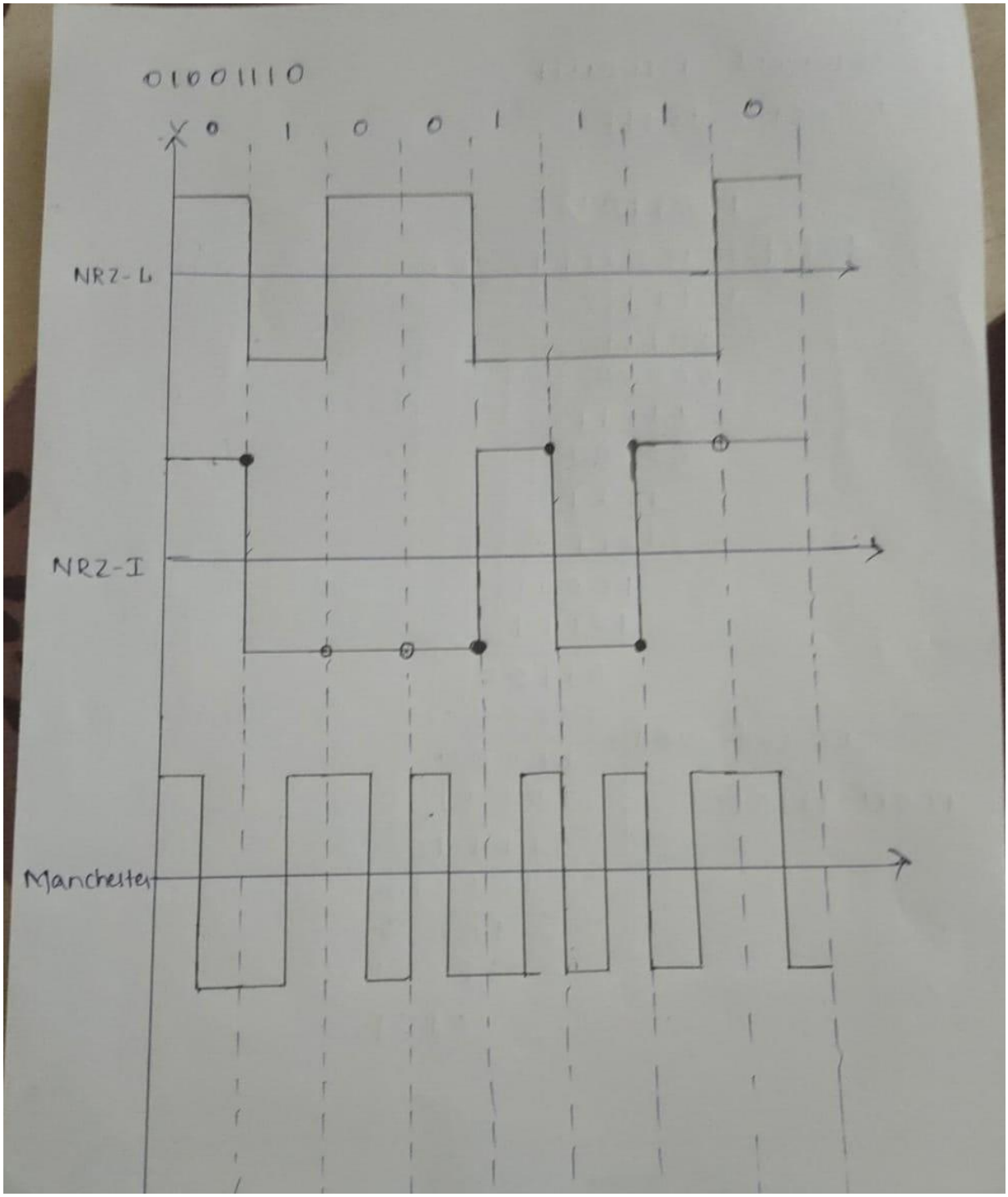
When the voltage level in a digital signal is constant for a while, the spectrum creates very low frequencies (results of Fourier analysis). These frequencies around zero, called DC (direct-current) components, present problems for a system that cannot pass low frequencies or a system that uses electrical coupling (via a transformer). We can say that DC component means 0/1 parity that can cause base-line wondering. For example, a telephone line cannot pass frequencies below 200 Hz. Also a long-distance link may use one or more transformers to isolate different parts of the line electrically. For these systems, we need a scheme with no DC component.

6. Self-synchronization
   To correctly interpret the signals received from the sender, the receiver's bit intervals must correspond exactly to the sender's bit intervals. If the receiver clock is faster or slower, the bit intervals are not matched and the receiver might misinterpret the signals. Figure 4.3 shows a situation in which the receiver has a shorter bit duration. The sender sends 10110001, while the receiver receives 110111000011.

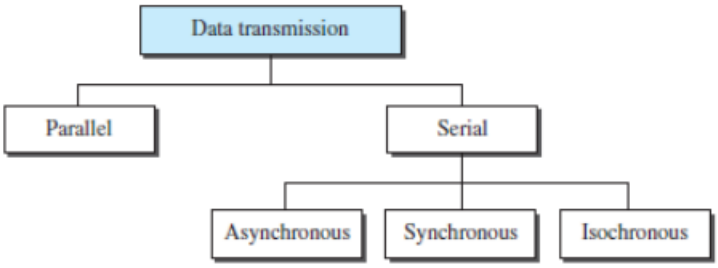


   A self-synchronizing digital signal includes timing information in the data being transmitted. This can be achieved if there are transitions in the signal that alert the receiver to the beginning, middle, or end of the pulse. If the receiver's clock is out of synchronization, these points can reset the clock.

7. Built-in Error Detection
   It is desirable to have a built-in error-detecting capability in the generated code to detect some or all of the errors that occurred during transmission.
8. Immunity to Noise and Interference
   Another desirable code characteristic is a code that is immune to noise and other interferences.
9. Complexity
   A complex scheme is more costly to implement than a simple one. For example, a scheme that uses four signal levels is more difficult to interpret than one that uses only two levels.



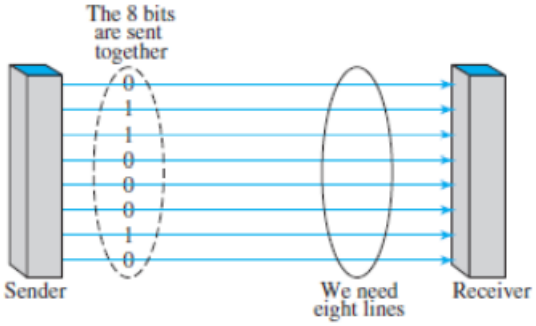
4b)



4.3.1 Parallel Transmission

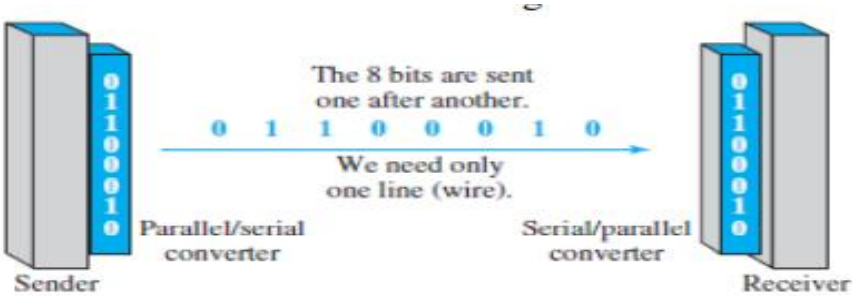
Binary data, consisting of 1s and 0s, may be organized into groups of n bits each. Computers produce and consume data in groups of bits much as we conceive of and use spoken language in the form of words rather than letters. By grouping, we can send data n bits at a time instead of 1. This is called parallel transmission.

The mechanism for parallel transmission is a conceptually simple one: Use n wires to send n bits at one time. That way each bit has its own wire, and all n bits of one group can be transmitted with each clock tick from one device to another. The next figure shows how parallel transmission works for n = 8. Typically, the eight wires are bundled in a cable with a connector at each end.



The advantage of parallel transmission is speed. All else being equal, parallel transmission can increase the transfer speed by a factor of n over serial transmission. But there is a significant disadvantage: cost. Parallel transmission requires n communication lines (wires in the example) just to transmit the data stream. Because this is expensive, parallel transmission is usually limited to short distances.

4.3.2 Serial Transmission In serial transmission one bit follows another, so we need only one communication channel rather than n to transmit data between two communicating devices.



The advantage of serial over parallel transmission is that with only one communication channel, serial transmission reduces the cost of transmission over parallel by roughly a factor of n.

Since communication within devices is parallel, conversion devices are required at the interface between the sender and the line (parallel-to-serial) and between the line and the receiver (serial-toparallel).

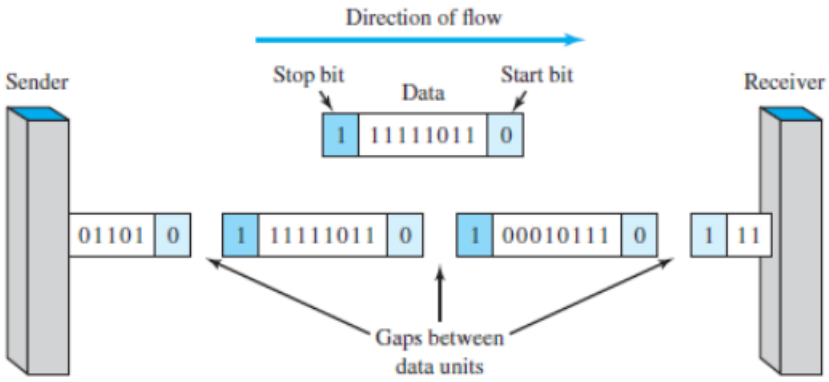
Serial transmission occurs in one of three ways: asynchronous, synchronous, and isochronous.

i. Asynchronous Transmission

Asynchronous transmission is so named because the timing of a signal is unimportant. Instead, information is received and translated by agreed upon patterns. As long as those patterns are followed, the receiving device can retrieve the information without regard to the rhythm in which it is sent. Patterns are based on grouping the bit stream into bytes. Each group, usually 8 bits, is sent along the link as a unit. The sending system handles each group independently, relaying it to the link whenever ready, without regard to a timer.

Without synchronization, the receiver cannot use timing to predict when the next group will arrive. To alert the receiver to the arrival of a new group, therefore, an extra bit is added to the beginning of each byte. This bit, usually a 0, is called the start bit. To let the receiver know that the byte is finished, 1 or more additional bits are appended to the end of the byte. These bits, usually 1s, are called stop bits. By this method, each byte is increased in size to at least 10 bits, of which 8 bits is information and 2 bits or more are signals to the receiver. In addition, the transmission of each byte may then be followed by a gap of varying duration. This gap can be represented either by an idle channel or by a stream of additional stop bits.

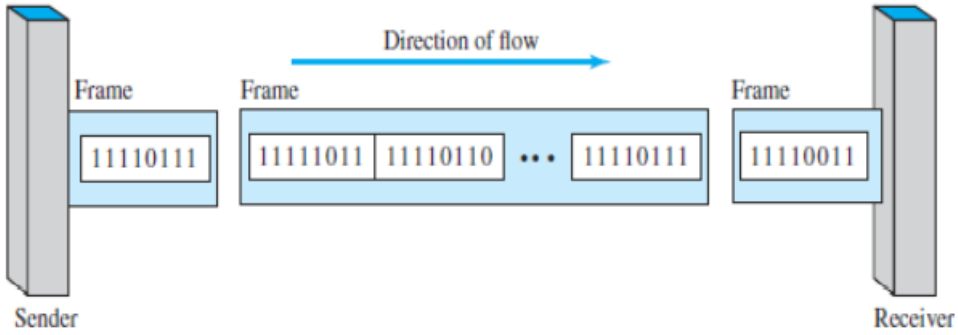
The start and stop bits and the gap alert the receiver to the beginning and end of each byte and allow it to synchronize with the data stream. This mechanism is called asynchronous because, at the byte level, the sender and receiver do not have to be synchronized. But within each byte, the receiver must still be synchronized with the incoming bit stream. That is, some synchronization is required, but only for the duration of a single byte. The receiving device resynchronizes at the onset of each new byte. When the receiver detects a start bit, it sets a timer and begins counting bits as they come in. After n bits, the receiver looks for a stop bit. As soon as it detects the stop bit, it waits until it detects the next start bit.



The above figure shows a schematic illustration of asynchronous transmission. In this example, the start bits are 0s, the stop bits are 1s, and the gap is represented by an idle line rather than by additional stop bits. The addition of stop and start bits and the insertion of gaps into the bit stream make asynchronous transmission slower than forms of transmission that can operate without the addition of control information. But it is cheap and effective, two advantages that make it an attractive choice for situations such as low-speed communication. For example, the connection of a keyboard to a computer is a natural application for asynchronous transmission. A user types only one character at a time, types extremely slowly in data processing terms, and leaves unpredictable gaps of time between characters.

ii. Synchronous Transmission

In synchronous transmission, the bit stream is combined into longer "frames," which may contain multiple bytes. Each byte, however, is introduced onto the transmission link without a gap between it and the next one. It is left to the receiver to separate the bit stream into bytes for decoding purposes. In other words, data are transmitted as an unbroken string of 1s and 0s, and the receiver separates that string into the bytes, or characters, it needs to reconstruct the information.



The above figure shows a schematic illustration of synchronous transmission. We have drawn in the divisions between bytes. In reality, those divisions do not exist; the sender puts its data onto the line as one long string. If the sender wishes to send data in separate bursts, the gaps between bursts must be filled with a special sequence of 0s and 1s that means idle. The receiver counts the bits as they arrive and groups them in 8-bit units.

Without gaps and start and stop bits, there is no built-in mechanism to help the receiving device adjust its bit synchronization midstream. Timing becomes very important, therefore, because the accuracy of the received information is completely dependent on the ability of the receiving device to keep an accurate count of the bits as they come in.

The advantage of synchronous transmission is speed. With no extra bits or gaps to introduce at the sending end and remove at the receiving end, and, by extension, with fewer bits to move across the link, synchronous transmission is faster than asynchronous transmission. For this reason, it is more useful for high-speed applications such as the transmission of data from one computer to another. Byte synchronization is accomplished in the data-link layer.

Although there is no gap between characters in synchronous serial transmission, there may be uneven gaps between frames.

iii. Isochronous

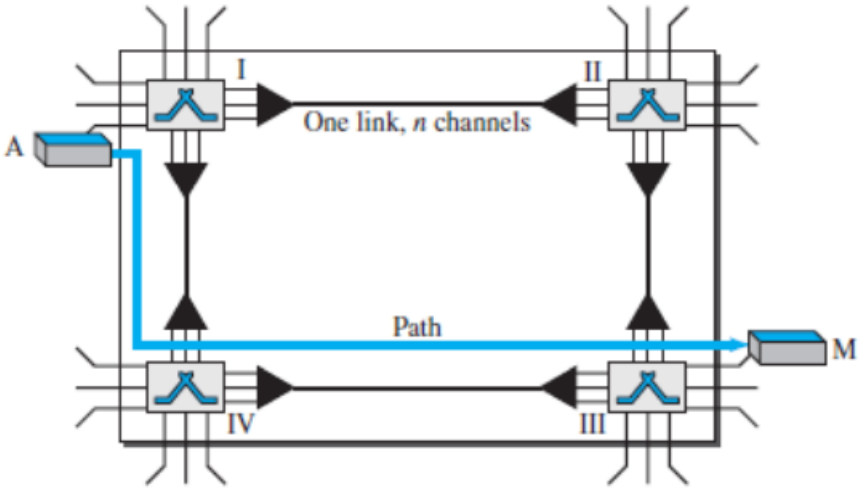
In real-time audio and video, in which uneven delays between frames are not acceptable, synchronous transmission fails. For example, TV images are broadcast at the rate of 30 images per second; they must be viewed at the same rate. If each image is sent by using one or more frames, there should be no delays between frames. For this type of application, synchronization between characters is not enough; the entire stream of bits must be synchronized. The isochronous transmission guarantees that the data arrive at a fixed rate.

4c)

In this example, S = 1000, N =8000, and rand L are unknown. We find first the value of rand then the value of L. S=Nx1/r r=N/S=8000/1000=8 bits/baud r= log2L L= 2 r = 2 8 =256

5a) Circuit-switched network consists of a set of switches connected by physical links.A connection between two stations is a dedicated path made of one or more links. However, each connection uses only one dedicated channel on each link. Each link is normally divided into n channels by using FDM or TDM.

Figure 8.3 *A trivial circuit-switched network*



We have explicitly shown the multiplexing symbols to emphasize the division of the link into channels even though multiplexing can be implicitly included in the switch fabric. The end systems, such as computers or telephones, are directly connected to a switch. We have shown only two end systems for simplicity. When end system A needs to communicate with end system M, system A needs to request a connection to M that must be accepted by all switches as well as by M itself. This is called the setup phase; a circuit (channel) is reserved on each link, and the combination of circuits or channels defines the dedicated path. After the dedicated path made of connected circuits (channels) is established, the data-transfer phase can take place. After all data have been transferred,the circuits are torn down.

We need to emphasize several points here:

- Circuit switching takes place at the physical layer.

- Before starting communication, the stations must make a reservation for the resources to be used during the communication. These resources, such as channels (bandwidth in FDM and time slots in TDM), switch buffers, switch processing time, and switch input/output ports, must remain dedicated during the entire duration of data transfer until the teardown phase.

- Data transferred between the two stations are not packetized (physical layer transfer of the signal). The data are a continuous flow sent by the source station and received by the destination station, although there may be periods of silence.

- There is no addressing involved during data transfer. The switches route the data based on their occupied band (FDM) or time slot (TDM). Of course, there is end-to-end addressing used during the setup phase.

8.2.1 Three Phases

The actual communication in a circuit-switched network requires three phases: connection setup, data transfer, and connection teardown.

1. Setup Phase
   Before the two parties (or multiple parties in a conference call) can communicate, a dedicated circuit (combination of channels in links) needs to be established. The end systems are normally connected through dedicated lines to the switches, so connection setup means creating dedicated channels between the switches. For example, in Figure 8.3,when system A needs to connect to system M, it sends a setup request that includes the address of system M, to switch I. Switch I finds a channel between itself and switch IV that can be dedicated for this purpose. Switch I then sends the request to switch IV, which finds a dedicated channel between itself and switch III. Switch III informs system M of system A's intention at this time. In the next step to making a connection, an acknowledgment from system M needs to be sent in the opposite direction to system A. Only after system A receives this acknowledgment is the connection established. Note that end-to-end addressing is required for creating a connection between the two end systems. These can be, for example, the addresses of the computers assigned by the administrator in a TDM network, or telephone numbers in an FDM network.
2. Data-Transfer Phase
   After the establishment of the dedicated circuit (channels), the two parties can transfer data.
3. Teardown Phase
   When one of the parties needs to disconnect, a signal is sent to each switch to release the resources.

5b)

Multiplexing is the set of techniques that allows the simultaneous transmission of multiple signals across a single data link.

6.1.2 Wavelength-Division Multiplexing

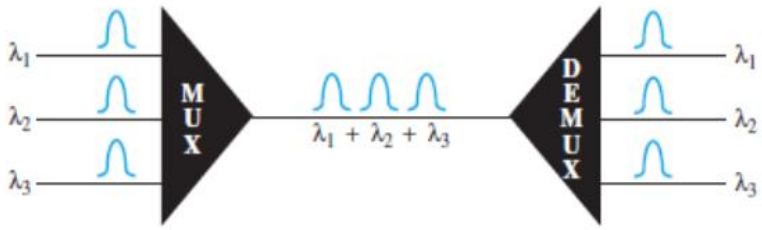
Wavelength-division multiplexing (WDM) is designed to use the high-data-rate capability of fiber-optic cable. The optical fiber data rate is higher than the data rate of metallic transmission cable. Using a fiber-optic cable for one single line wastes the available bandwidth. Multiplexing allows us to combine several lines into one.

WDM is conceptually the same as FDM, except that the multiplexing and demultiplexing involve optical signals transmitted through fiber-optic channels. The idea is the same: We are combining different signals of different frequencies. The difference is that the frequencies are very high.

Figure 6.10 gives a conceptual view of a WDM multiplexer and demultiplexer. Very narrow bands of light from different sources are combined to make a wider band of light. At the receiver, the signals are separated by the demultiplexer

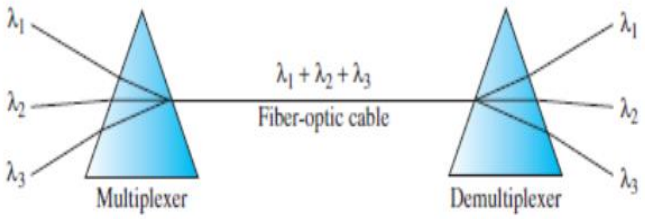
Figure 6.10 *Wavelength-division multiplexing*

Figure 6.10 *Wavelength-division multiplexing*



Although WDM technology is very complex, the basic idea is very simple. We want to combine multiple light sources into one single light at the multiplexer and do the reverse at the demultiplexer. The combining and splitting of light sources are easily handled by a prism. Recall from basic physics that a prism bends a beam of light based on the angle of incidence and the frequency. Using this technique, a multiplexer can be made to combine several input beams of light, each containing a narrow band of frequencies, into one output beam of a wider band of frequencies. A demultiplexer can also be made to reverse the process. Figure 6.11 shows the concept.

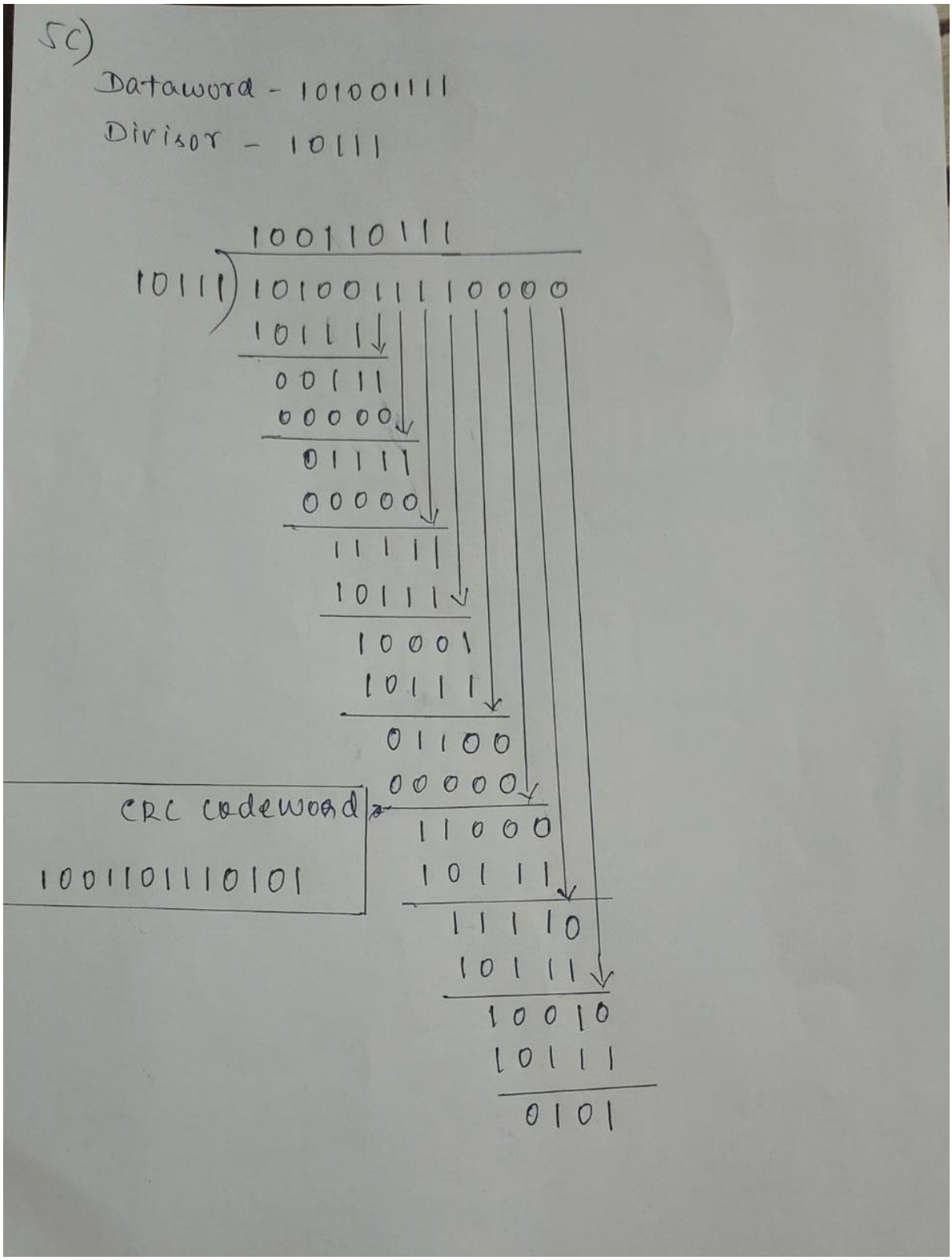
Figure 6.11 *Prisms in wavelength-division multiplexing and demultiplexing*



One application of WDM is the SONET network, in which multiple optical fiber lines are multiplexed and demultiplexed. A new method, called dense WDM (DWDM), can multiplex a

very large number of channels by spacing channels very close to one another. It achieves even greater efficiency.

5c)



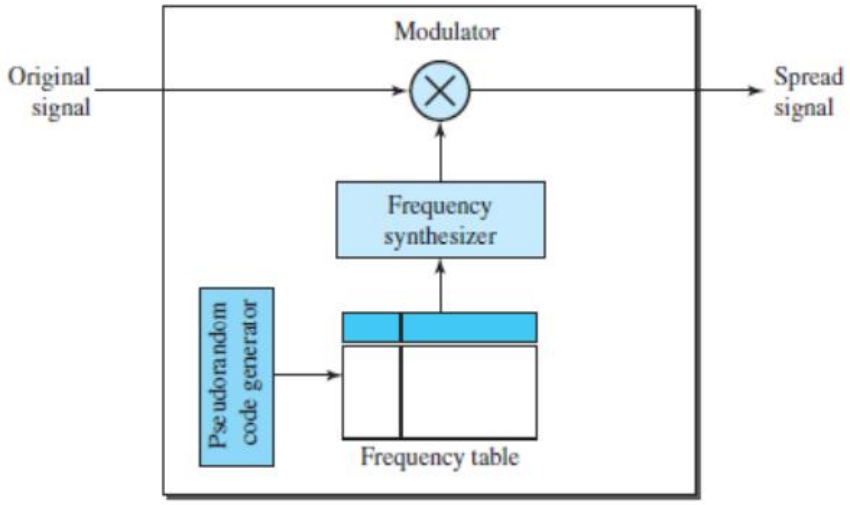
6a)

Multiplexing combines signals from several sources to achieve bandwidth efficiency; the available bandwidth of a link is divided between the sources. In spread spectrum, we also combine signals from different sources to fit into a larger bandwidth, but our goals are somewhat different. Spread spectrum is designed to be used in wireless applications(LANs and WANs).

6.2.1 Frequency Hopping Spread Spectrum (FHSS)

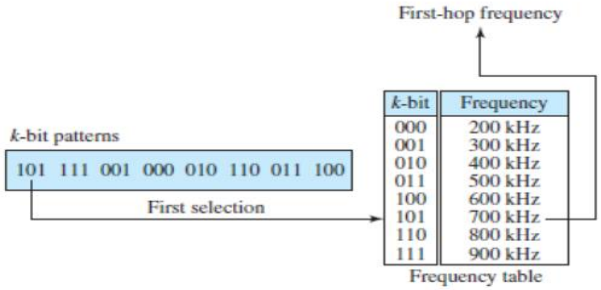
The frequency hopping spread spectrum (FHSS) technique uses M different carrier frequencies that are modulated by the source signal. At one moment, the signal modulates one carrier frequency; at the next moment, the signal modulates another carrier frequency. Although the modulation is done using one carrier frequency at a time, M frequencies are used in the long run. The bandwidth occupied by a source after spreading is BpHSS »B. Figure 6.28 shows the general layout for FHSS. A pseudorandom code generator, called pseudorandom noise (PN), creates a k-bit pattern for every hopping period Th• The frequency table uses the pattern to find the frequency to be used for this hopping period and passes it to the frequency synthesizer. The frequency synthesizer creates a carrier signal of that frequency, and the source signal modulates the carrier signal.

Figure 6.28 *Frequency hopping spread spectrum (FHSS)*



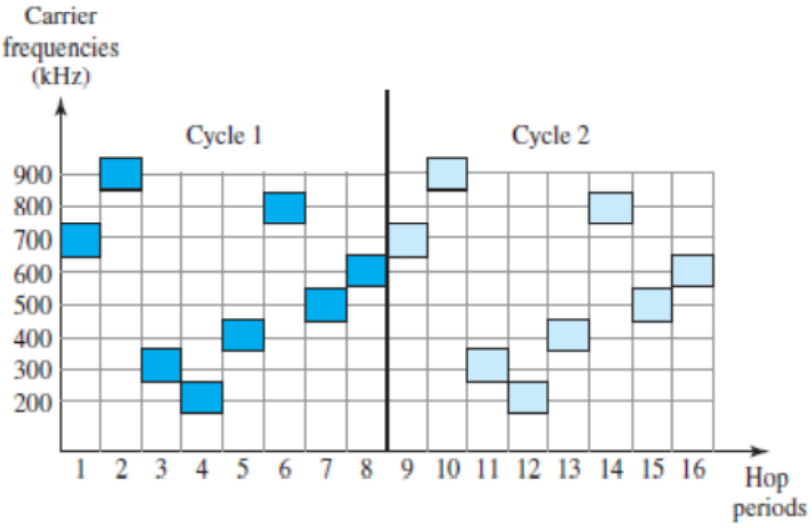
Suppose we have decided to have eight hopping frequencies. This is extremely low for real applications and is just for illustration. In this case, M is 8 and k is 3. The pseudorandom code generator will create eight different 3-bit patterns. These are mapped to eight different frequencies in the frequency table (see Figure 6.29).

Figure 6.29 *Frequency selection in FHSS*



The pattern for this station is 101, 111, 001, 000, 010, all, 100. Note that the pattern is pseudorandom it is repeated after eight hoppings. This means that at hopping period 1, the pattern is 101. The frequency selected is 700 kHz; the source signal modulates this carrier frequency. The second k-bit pattern selected is 111, which selects the 900-kHz carrier; the eighth pattern is 100, the frequency is 600 kHz. After eight hoppings, the pattern repeats, starting from 101 again. Figure 6.30 shows how the signal hops around from carrier to carrier. We assume the required bandwidth of the original signal is 100 kHz.

Figure 6.30 *FHSS cycles*

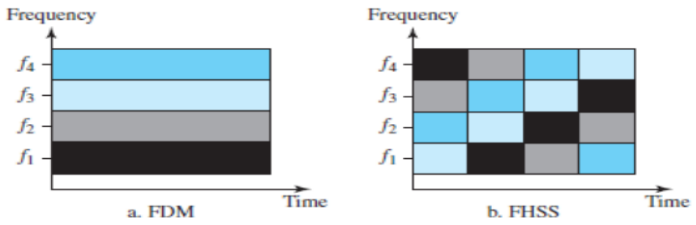


It can be shown that this scheme can accomplish the previously mentioned goals. If there are many k-bit patterns and the hopping period is short, a sender and receiver can have privacy. If an intruder tries to intercept the transmitted signal, she can only access a small piece of data because she does not know the spreading sequence to quickly adapt herself to the next hop. The scheme has also an antijamming effect. A malicious sender may be able to send noise to jam the signal for one hopping period (randomly), but not for the whole period.

If the number of hopping frequencies is M, we can multiplex M channels into one by using the same Bss bandwidth. This is possible because a station uses just one frequency in each hopping period; M - 1 other frequencies can be used by other M - 1 stations. In other words, M different stations can use the same Bss if an appropriate modulation technique such as multiple FSK

(MFSK) is used. FHSS is similar to FDM, as shown in Figure 6.31.Figure 6.31 shows an example of four channels using FDM and four channels using FHSS.

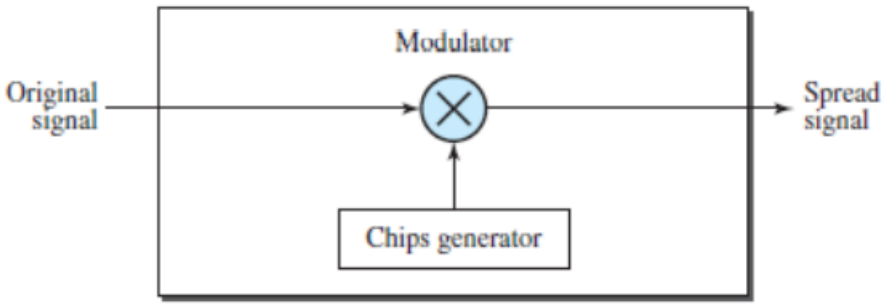
Figure 6.31 *Bandwidth sharing*



6.2.2 Direct Sequence Spread Spectrum

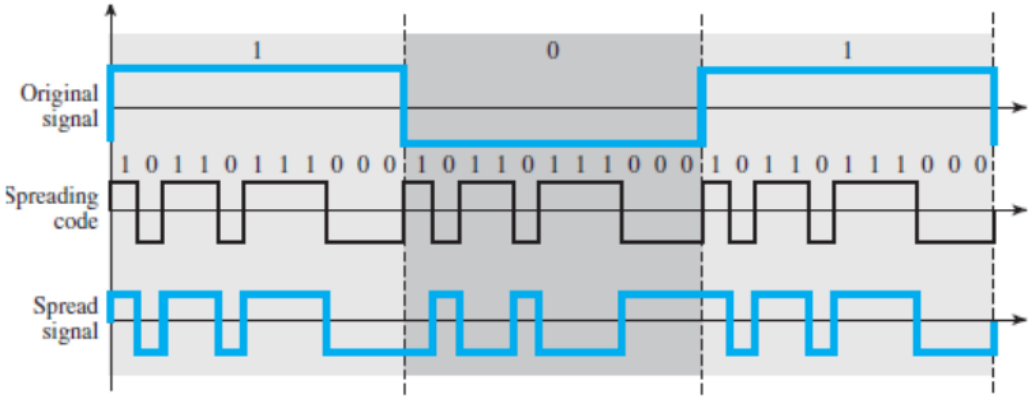
The direct sequence spread spectrum (nSSS) technique also expands the bandwidth of the original signal, but the process is different. In DSSS, we replace each data bit with 11 bits using a spreading code. In other words, each bit is assigned a code of 11 bits, called chips, where the chip rate is 11 times that of the data bit. Figure 6.32 shows the concept of DSSS.

Figure 6.32 *DSSS*



As an example, let us consider the sequence used in a wireless LAN, the famous Barker sequence where n is 11. We assume that the original signal and the chips in the chip generator use polar NRZ encoding. Figure 6.33 shows the chips and the result of multiplying the original data by the chips to get the spread signal.

Figure 6.33 *DSSS example*



In Figure 6.33, the spreading code is 11 chips having the pattern 10110111000 (in this case). If the original signal rate is N, the rate of the spread signal is lIN. This means that the required bandwidth for the spread signal is 11 times larger than the bandwidth of the original signal. The spread signal can provide privacy if the intruder does not know the code. It can also provide immunity against interference if each station uses a different code.

7a)

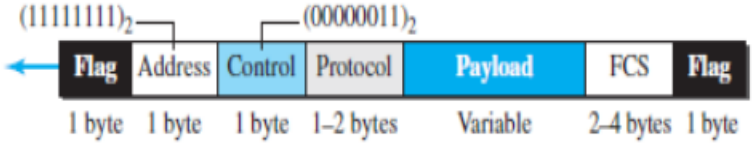
POINT-TO-POINT PROTOCOL (PPP)

One of the most common protocols for point-to-point access is the Point-to-Point Protocol (PPP). Today, millions of Internet users who need to connect their home computers to the server of an Internet service provider use PPP. The majority of these users have a traditional modem; they are connected to the Internet through a telephone line, which provides the services of the physical layer. But to control and manage the transfer of data, there is a need for a point-to-point protocol at the data-link layer. PPP is by far the most common.

Framing

PPP uses a character-oriented (or byte-oriented) frame. Figure shows the format of a PPP frame. The description of each field follows:

Figure 11.20 *PPP frame format*



Flag

A PPP frame starts and ends with a 1-byte flag with the bit pattern 01111110.

Address

The address field in this protocol is a constant value and set to 11111111 (broadcast address

Control

This field is set to the constant value 00000011. PPP does not provide any flow control. Error control is also limited to error detection.

Protocol

The protocol field defines what is being carried in the data field: either user data or other information. This field is by default 2 bytes long, but the two parties can agree to use only 1 byte.

Payload field

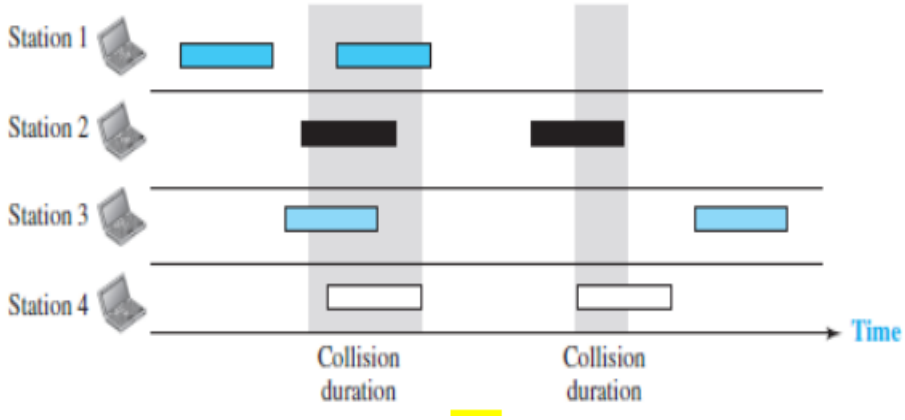
This field carries either the user data or other information. The data field is a sequence of bytes with the default of a maximum of 1500 bytes; but this can be changed during negotiation. The data field is bytestuffed if the flag byte pattern appears in this field. Because there is no field defining the size of the data field, padding is needed if the size is less than the maximum default value or the maximum negotiated value.

FCS

The frame check sequence (FCS) is simply a 2-byte or 4-byte standard CRC.

7b)

Pure ALOHA The idea is that each station sends a frame whenever it has a frame to send (multiple access). However, since there is only one channel to share, there is the possibility of collision between frames from different stations.



For example, consider the above example of a pure ALOHA network. There are four stations that contend with one another for access to the shared channel. The figure shows that each station sends two frames; there are a total of eight frames on the shared medium. Some of these frames collide because multiple frames are in contention for the shared channel. The figure shows that only two frames survive: one frame from station 1 and one frame from station 3. (We need to mention that even if one bit of a frame coexists on the channel with one bit from another frame, there is a collision and both will be destroyed.) So, it is obvious that we need to resend the frames that have been destroyed during transmission.

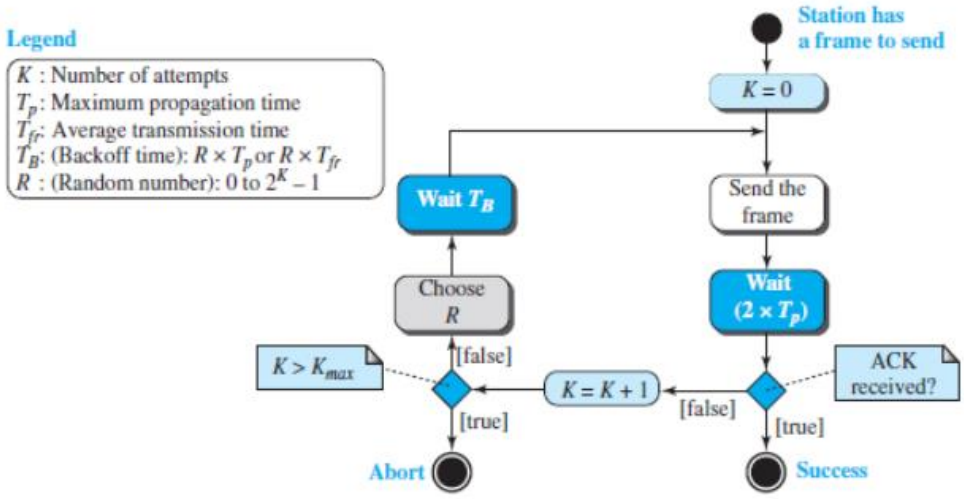
Here is how Pure ALOHA works: • The sender sends a frame & starts the timer. • The receiver receives the frame and responds with an acknowledgment. • If the acknowledgment does not arrive after a time-out period, the sender resends the frame as the sender assumes that the frame (or the acknowledgment) has been destroyed. • Since the medium is shared between the stations, there is the possibility of collisions. • If two stations try to resend the frames after the time-out, the frames will collide again. • There are two methods to deal with collision:

Randomness

When the time-out period passes, each station waits a random amount of time before resending the frame. This time is called back-off time TB. The randomness will help avoid more collisions.

Limit Maximum Retransmission

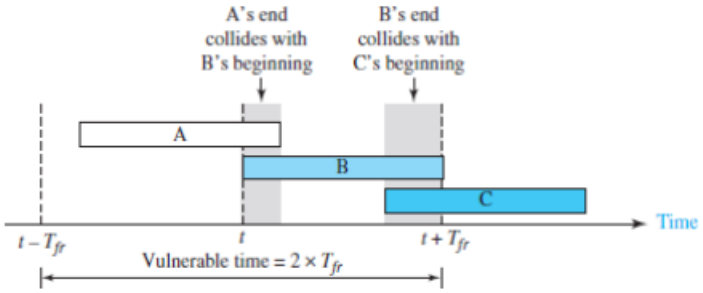
This method prevents congestion by reducing the number of retransmitted frames. After a maximum number of retransmission attempts Kmax, a station must give up and try later.



Vulnerable time • The vulnerable-time is defined as a time during which there is a possibility of collision.

Pure Aloha vulnerable time=2*Tfr

where Tfr = Frame transmission time



In Figure, If station B sends a frame between t-Tfr and t, this leads to a collision between the frames from station A and station B. If station C sends a frame between t and t+Tfr, this leads to a collision between the frames from station A and station C.

Throughput

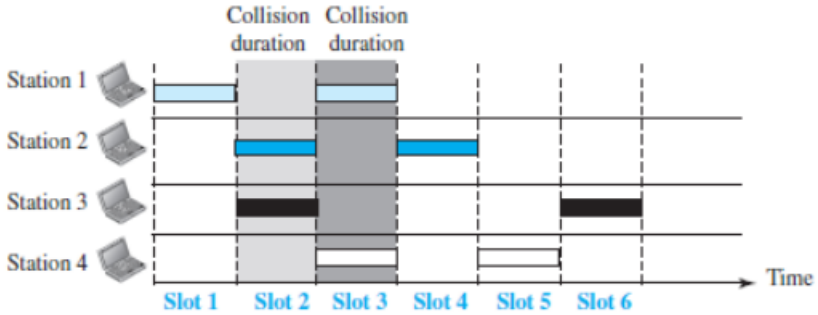
• The average number of successful transmissions is given by

$$S = G \times e^{-2G}$$

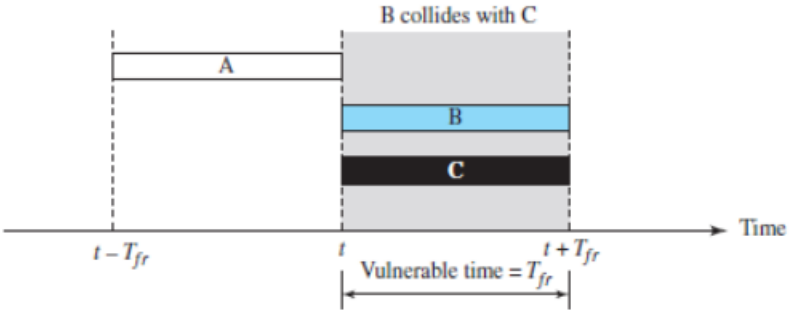
where G = average no. of frames in one frame transmission time (Tfr) For G = 1, the maximum throughput Smax = 0.184. In other words, out of 100 frames, 18 frames reach their destination successfully.

Slotted ALOHA

Slotted ALOHA was invented to improve the efficiency of pure ALOHA. The time is divided into time-slots of Tfr seconds (Figure 12.5). The stations are allowed to send only at the beginning of the time-slot.



If a station misses the time-slot, the station must wait until the beginning of the next time-slot. If 2 stations try to resend at beginning of the same time-slot, the frames will collide again (Fig 12.6).



• The vulnerable time is given by:

Slotted Aloha vulnerable time=Tfr

Throughput

The average number of successful transmissions is given by

$$S = G \times e^{-G}.$$

For G = 1, the maximum throughput Smax = 0.368. In other words, out of 100 frames, 36 frames reach their destination successfully.

7c)

Stop-and-Wait Protocol

1. Second protocol is called the Stop-and-Wait protocol, which uses both flow and error control. 2. In this protocol, the sender sends one frame at a time and waits for an

acknowledgment before sending the next one. 3. To detect corrupted frames, we need to add a CRC to each data frame. 4. When a frame arrives at the receiver site, it is checked. If its CRC is incorrect, the frame is corrupted and silently discarded. 5. The silence of the receiver is a signal for the sender that a frame was either corrupted or lost. 6. Every time the sender sends a frame, it starts a timer. If an acknowledgment arrives before the timer expires, the timer is stopped and the sender sends the next frame (if it has one to send). 7. If the timer expires, the sender resends the previous frame, assuming that the frame was either lost or corrupted. 8. This means that the sender needs to keep a copy of the frame until its acknowledgment arrives. 9. When the corresponding acknowledgment arrives, the sender discards the copy and sends the next frame if it is ready. 10. Figure shows the outline for the Stop-and-Wait protocol. 11. Note that only one frame and one acknowledgment can be in the channels at any time.

Figure 11.10 *Stop-and-Wait protocol*

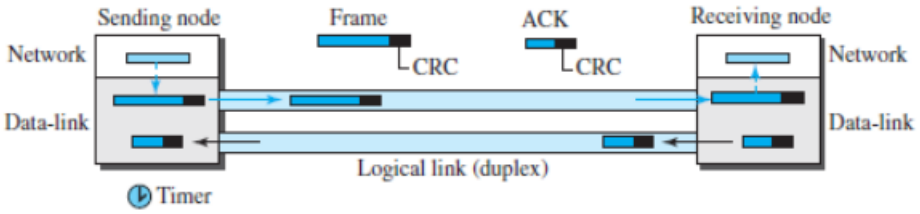
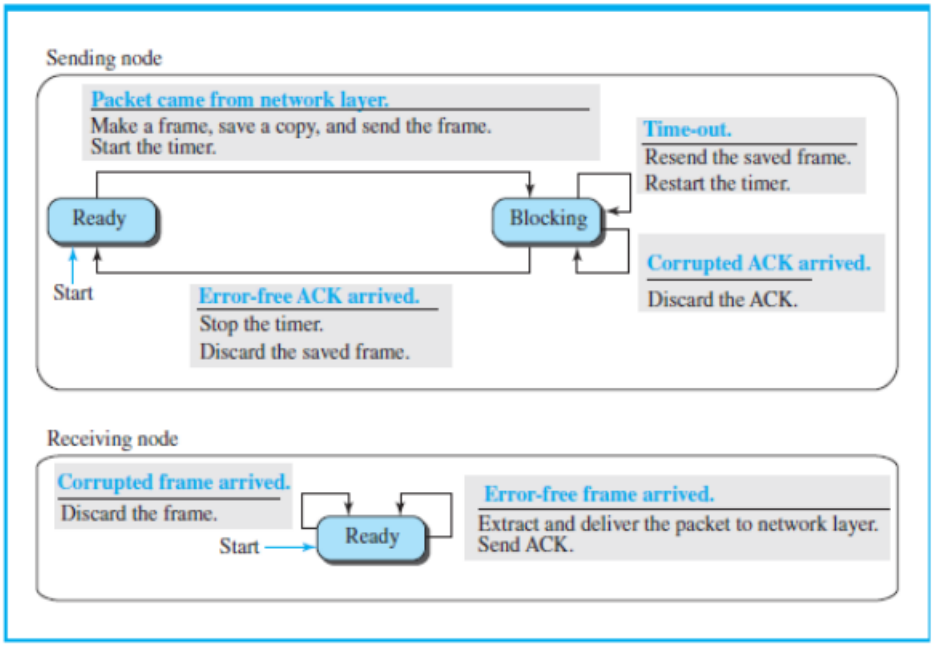


Figure 11.11 shows the FSMs for our primitive Stop-and-Wait protocol.

Figure 11.11 *FSM for the Stop-and-Wait protocol*



We describe the sender and receiver states below.

Sender States

The sender is initially in the Ready state, but it can move between the Ready and Blocking state.

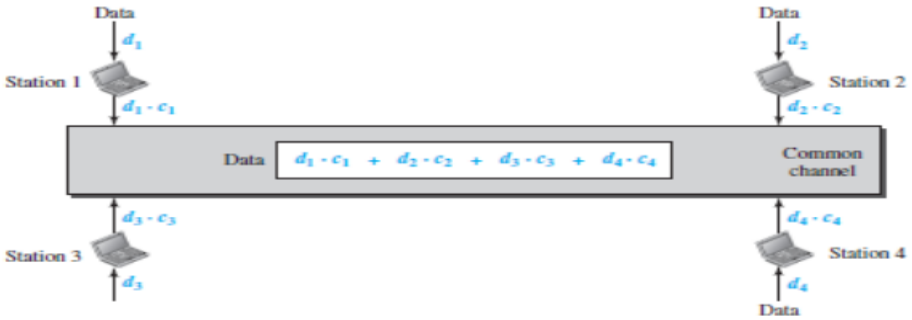
1. Ready State • When the sender is in this state, it is only waiting for a packet from the network layer. • If a packet comes from the network layer, the sender creates a frame, saves a copy of the frame, starts the timer and sends the frame. • The sender then moves to the Blocking state.
2. Blocking State: When the sender is in this state, three events can occur • If a time-out occurs, the sender resends the saved copy of the frame and restarts the timer. • If a corrupted ACK arrives, it is discarded. • If an error-free ACK arrives, the sender stops the timer and discards the saved copy of the frame. It then moves to the Ready state.

Receiver States
The receiver is always in the Ready state. Two events may occur: • If an error-free frame arrives, the message in the frame is delivered to the network layer and an ACK is sent. • If a corrupted frame arrives, the frame is discarded.

8a)
CHANNELIZATION PROTOCOLS
Channelization is a multiple-access method. The available bandwidth of a link is shared b/w different stations in time, frequency, or through code. Three channelization protocols: FDMA (Frequency Division Multiple Access) TDMA (Time Division Multiple Access) and CDMA (Code Division Multiple Access)

CDMA
CDMA simply means communication with different codes. CDMA differs from FDMA because only one channel occupies the entire bandwidth of the link. CDMA differs from TDMA because all stations can send data simultaneously; there is no timesharing. (Analogy: CDMA simply means communication with different codes. For example, in a large room with many people, 2 people can talk privately in English if nobody else understands English. Another 2 people can talk in Chinese if they are the only ones who understand Chinese, and so on).

Implementation
Let us assume we have four stations 1, 2, 3, and 4 connected to the same channel. The data from station-1 are d1, from station-2 are d2, and so on. The code assigned to the first station is c1, to the second is c2, and so on. We assume that the assigned codes have 2 properties. If we multiply each code by another, we get 0. If we multiply each code by itself, we get 4 (the number of stations).



Here is how it works: Station-1 multiplies the data by the code to get d1.c1. Station-2 multiplies the data by the code to get d2.c2. And so on. The data that go on the channel are the sum of all these terms. The receiver multiplies the data on the channel by the code of the sender. For example, suppose stations 1 and 2 are talking to each other. Station-2 wants to hear what station-1 is saying. Station-2 multiplies the data on the channel by c1 the code of station-1. (c1.c1)=4, (c2.c1)=0, (c3.c1)=0, and (c4.c1)=0, Therefore, station-2 divides the result by 4 to get the data from station-1.

$$\begin{aligned}\text{data} &= (d_1 \cdot c_1 + d_2 \cdot c_2 + d_3 \cdot c_3 + d_4 \cdot c_4) \cdot c_1 \\ &= d_1 \cdot c_1 \cdot c_1 + d_2 \cdot c_2 \cdot c_1 + d_3 \cdot c_3 \cdot c_1 + d_4 \cdot c_4 \cdot c_1 = 4 \times d_1\end{aligned}$$

Chips CDMA is based on coding theory. Each station is assigned a code, which is a sequence of numbers called chips (Figure 12.24).

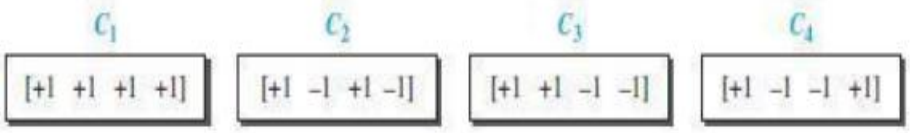
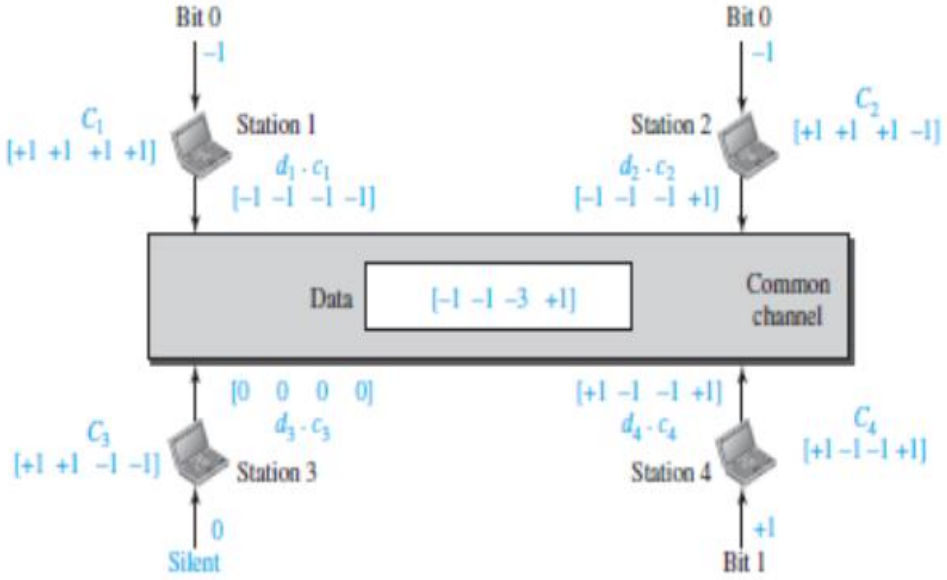


Figure 12.24 *Chip sequences*

These sequences were carefully selected & are called orthogonal sequences These sequences have the following properties: Each sequence is made of N elements, where N is the number of stations.
Multiplication of a sequence by a scalar: If we multiply a sequence by a number i.e. every element in the sequence is multiplied by that element. For example,
3) Inner product of 2 equal sequences: If we multiply 2 equal sequences, element by element, and add the results, we get N, where N is the number of elements in the each sequence.
4) Inner product of 2 different sequences: If we multiply 2 different sequences, element by element, and add the results, we get 0.
5) Adding 2 sequences means adding the corresponding elements. The result is another sequence.

Data Representation
We follow the following rules for encoding: To send a 0 bit, a station encodes the bit as -1 To send a 1 bit, a station encodes the bit as +1 When a station is idle, it sends no signal, which is interpreted as a 0.

Encoding and Decoding
We assume that Stations 1 and 2 are sending a 0 bit. Station-4 is sending a 1 bit. Station-3 is silent. Here is how it works (Figure 12.26): At the sender-site, the data are translated to -1, -1, 0, and +1. Each station multiplies the corresponding number by its chip (its orthogonal sequence). The result is a new sequence which is sent to the channel. The sequence on the channel is the sum of all 4 sequences. Now imagine station3, which is silent, is listening to station-2. Station-3 multiplies the total data on the channel by the code for station-2, which is [+1 -1 +1- 1], to get



8b)

CONTROLLED ACCESS PROTOCOLS

Here, the stations consult one another to find which station has the right to send. A station cannot send unless it has been authorized by other stations. Three popular controlled-access methods are: 1) Reservation 2) Polling 3) Token Passing

Token Passing

In a network, the stations are organized in a ring fashion i.e. for each station; there is a predecessor and a successor. The predecessor is the station which is logically before the station in the ring. The successor is the station which is after the station in the ring. The current station is the one that is accessing the channel now. A token is a special packet that circulates through the ring. Here is how it works: A station can send the data only if it has the token. When a station wants to send the data, it waits until it receives the token from its predecessor. Then, the station holds the token and sends its data. When the station finishes sending the data, the station releases the token passes the token to the successor. Main functions of token management: Stations must be limited in the time they can hold the token. The token must be monitored to ensure it has not been lost or destroyed. For ex: if a station that is holding the token fails, the token will disappear from the network Assign priorities to the stations and to the types of data being transmitted. Make low-priority stations release the token to high priority stations.

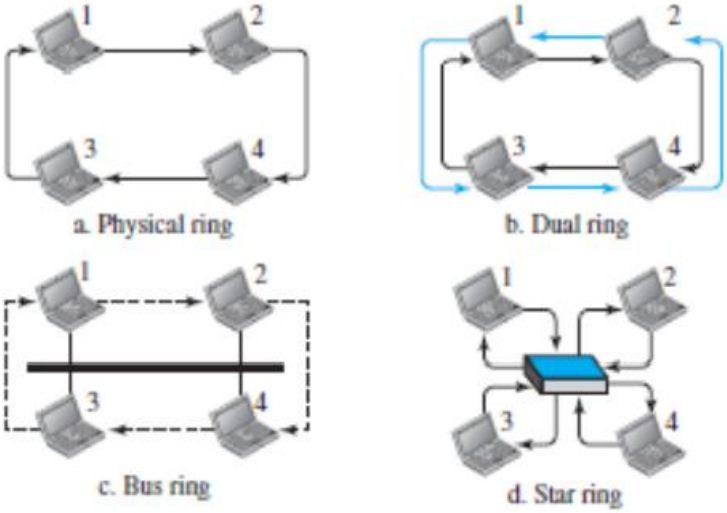
Logical Ring In a token-passing network, stations do not have to be physically connected in a ring; the ring can be a logical one. Four physical topologies to create a logical ring (Figure 12.20):

Physical ring

Dual ring

Bus ring

Star ring



1) Physical Ring Topology
   When a station sends token to its successor, token cannot be seen by other stations. (Figure a) This means that the token does not have the address of the next successor. Disadvantage: If one of the links fails, the whole system fails.
2) Dual Ring Topology
   • A second (auxiliary) ring → is used along with the main ring (Figure b). → operates in the reverse direction compared with the main ring. → is used for emergencies only (such as a spare tire for a car). • If the main ring fails, the system automatically combines the 2 rings to form a temporary ring. • After the failed link is restored, the second ring becomes idle again. • Each station needs to have 2 transmitter-ports and 2 receiver-ports. • This topology is used in i)FDDI (Fiber Distributed Data Interface) and ii) CDDI (Copper Distributed Data Interface).
3) Bus Ring Topology
   • The stations are connected to a single cable called a bus (Figure c). • This makes a logical ring, because each station knows the address of its successor and predecessor. • When a station has finished sending its data, the station → releases the token and → inserts the address of its successor in the token. • Only the station gets the token to access the shared media. • This topology is used in the Token Bus LAN.
4) Star Ring Topology
   The physical topology is a star (Figure d). There is a hub that acts as the connector. The wiring inside the hub makes the ring i.e. the stations are connected to the ring through the 2 wire connections. Disadvantages: This topology is less prone to failure because If a link goes down, then the link will be bypassed by the hub and the rest of the stations can operate. Also adding and removing stations from the ring is easier. This topology is used in the Token Ring LAN.

8c)

Classful Addressing

When the Internet started, an IPv4 address was designed with a fixed-length prefix, but to accommodate both small and large networks, three fixed-length prefixes were designed instead of one (n = 8, n = 16, and n = 24). The whole address space was divided into five classes (class A, B, C, D, and E), as shown in the below figure. This scheme is referred to as classful addressing.

In class A, the network length is 8 bits, but since the first bit, which is 0, defines the class, we can have only seven bits as the network identifier. This means there are only $2^7 = 128$ networks in the world that can have a class A address.

In class B, the network length is 16 bits, but since the first two bits, which are $(10)_2$, define the class, we can have only 14 bits as the network identifier. This means there are only $2^{14} = 16,384$ networks in the world that can have a class B address.

All addresses that start with $(110)_2$ belong to class C. In class C, the network length is 24 bits, but since three bits define the class, we can have only 21 bits as the network identifier. This means there are $2^{21} = 2,097,152$ networks in the world that can have a class C address.

Class D is not divided into prefix and suffix. It is used for multicast addresses. All addresses that start with 1111 in binary belong to class E. As in Class D, Class E is not divided into prefix and suffix and is used as reserve.

Address Depletion

The reason that classful addressing has become obsolete is address depletion. Since the addresses were not distributed properly, the Internet was faced with the problem of the addresses being rapidly used up, resulting in no more addresses available for organizations and individuals that needed to be connected to the Internet. To understand the problem, let us think about class A. This class can be assigned to only 128 organizations in the world, but each organization needs to have a single network (seen by the rest of the world) with 16,777,216 nodes (computers in this single network). Since there may be only a few organizations that are this large, most of the addresses in this class were wasted (unused). Class B addresses were designed for midsize organizations, but many of the addresses in this class also remained unused. Class C addresses have a completely different flaw in design. The number of addresses that can be used in each network (256) was so small that most companies were not comfortable using a block in this address class. Class E addresses were almost never used, wasting the whole class.

Subnetting and Supernetting

To alleviate address depletion, two strategies were proposed and, to some extent, implemented: subnetting and supernetting. In subnetting, a class A or class B block is divided into several subnets. Each subnet has a larger prefix length than the original network. For example, if a network in class A is divided into four subnets, each subnet has a prefix of $n_{sub} = 10$. At the same time, if all of the addresses in a network are not used, subnetting allows the addresses to be divided among several organizations. This idea did not work because most large organizations were not happy about dividing the block and giving some of the unused addresses to smaller organizations.

While subnetting was devised to divide a large block into smaller ones, supernetting was devised to combine several class C blocks into a larger block to be attractive to organizations that need more than the 256 addresses available in a class C block. This idea did not work either because it makes the routing of packets more difficult.

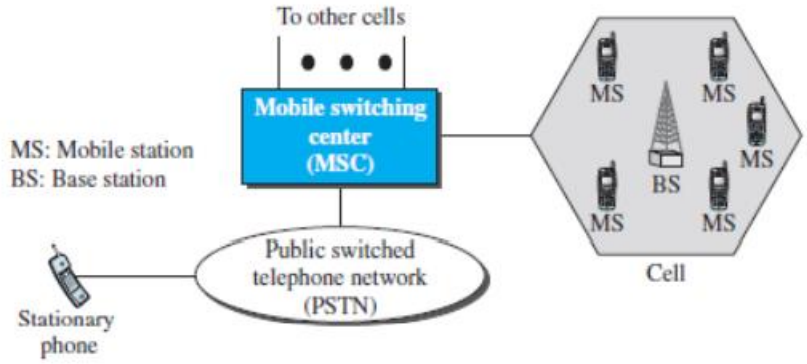
9a)

CELLULAR TELEPHONY

Cellular telephony is designed to provide communications between two moving units called mobile-stations (MSs) or between one mobile-station and one stationary unit called a land unit .

A service-provider is responsible for locating & tracking a caller assigning a channel to the call and transferring the channel from base-station to base-station as the caller moves out-of-range. Each cellular service-area is divided into small regions called cells. Each cell contains an antenna. Each cell is controlled by AC powered network-station called the base-station (BS). Each base-station is controlled by a switching office called a mobile-switchingcenter (MSC). MSC coordinates communication between all the base-stations and the telephone central office. MSC is a computerized center that is

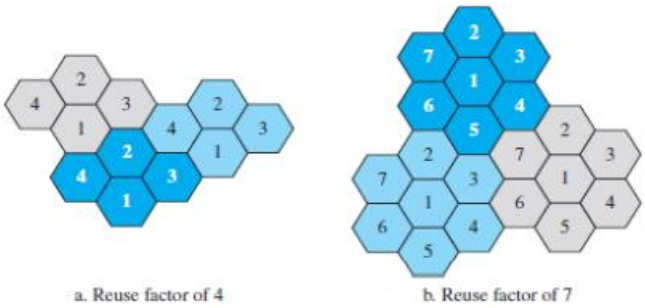
responsible for connecting calls recording call information and billing. Cell-size is not fixed; Cell-size can be increased or decreased depending on population of the area. Cell-radius = 1 to 12 mi. Compared to low-density areas, high-density areas require many smaller cells to meet traffic demands. Cell-size is optimized to prevent the interference of adjacent cell-signals.



Operation

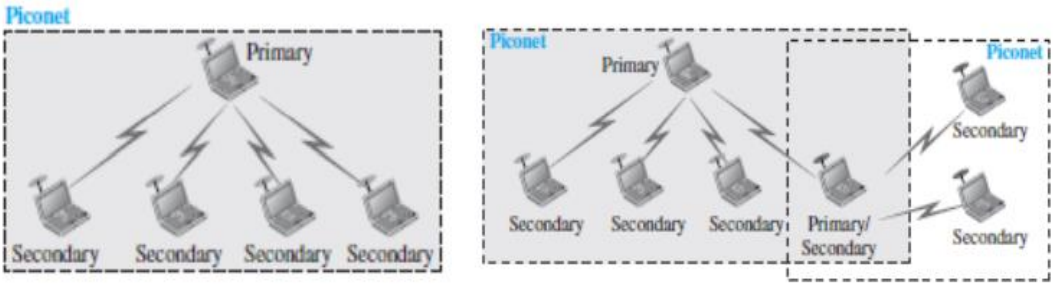
Frequency-Reuse Principle

In general, neighboring-cells cannot use the same set of frequencies for communication. Using same set of frequencies may create interference for the users located near the cell-boundaries. However, set of frequencies available is limited and frequencies need to be reused. A frequency reuse pattern is a configuration of N cells. Where N = reuse factor Each cell uses a unique set of frequencies. When the pattern is repeated, the frequencies can be reused. There are several different patterns (Figure 16.7). The numbers in the cells define the pattern. The cells with the same number in a pattern can use the same set of frequencies. These cells are called the reusing cells.



9b) Architecture

Bluetooth defines 2 types of networks: 1) Piconet and 2) Scatternet. Piconets A Bluetooth network is called a piconet, or a small net. (Figure 15.17). A piconet can have up to 8 stations. Out of which One of station is called the primary. The remaining stations are called secondaries. All the secondary-stations synchronize their clocks and hopping sequence with the primary station. A piconet can have only one primary station. The communication between the primary and the secondary can be one-to-one or one-to-many.



Although a piconet can have a maximum of 7 secondaries, an additional 8 secondaries can be in the parked state. A secondary in a parked state is synchronized with the primary, but cannot take part in communication until it is moved from the parked state. Because only 8 stations can be active in a piconet, activating a station from the parked state means that an active station must go to the parked state. Scatternet Piconets can be combined to form a scatternet. A station can be a member of 2 piconets. A secondary station in one piconet can be the primary in another piconet. This is called mediator station. Acting as a secondary, mediator station can receive messages from the primary in the first piconet. Acting as a primary, mediator station can deliver the message to secondaries in the second piconet.

9c)

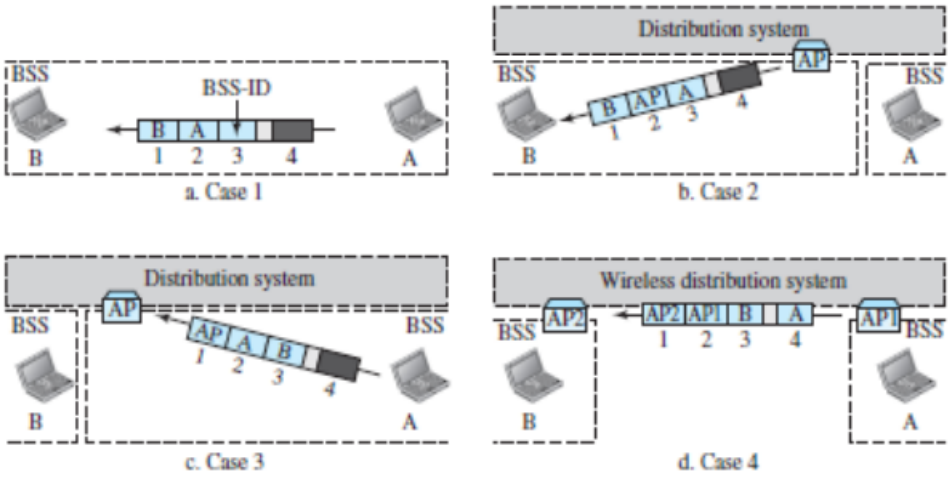
Addressing Mechanism The IEEE 802.11 addressing mechanism specifies 4 cases, defined by the value of the 2 flags in the FC field, To DS and From DS. (DS stands for Distribution System). Each flag can be either 0 or 1, resulting in 4 different situations. The interpretation of the 4 addresses (address 1 to address 4) in the MAC frame depends on the value of these flags, as shown in the Table.

To DS	*From DS*	*Address 1*	*Address 2*	*Address 3*	*Address 4*
0	0	Destination	Source	BSS ID	N/A
0	1	Destination	Sending AP	Source	N/A
1	0	Receiving AP	Source	Destination	N/A
1	1	Receiving AP	Sending AP	Destination	Source

Address 1 is always the address of the next device. Address 2 is always the address of the previous device. Address 3 is the address of the final destination-station if it is not defined by address 1. Address 4 is the address of the original source-station if it is not the same as address 2.

Case-1: 00

In this case, To DS = 0 and From DS = 0 (Figure a). This means that the frame is not going to a distribution-system (To DS = 0) and is not coming from a distribution-system (From DS = 0). The frame is going from one station in a BSS to another without passing through the distribution-system. The ACK frame should be sent to the original sender.



Case-2: 01

In this case, To DS = 0 and From DS = 1 (Figure b). This means that the frame is coming from a distribution-system (From DS = 1). The frame is coming from an AP and going to a station. The ACK should be sent to the AP. The address 3 contains the original sender of the frame (in another BSS).

Case-3: 10

In this case, To DS = 1 and From DS = 0 (Figure c). This means that the frame is going to a distribution-system (To DS = 1). The frame is going from a station to an AP. The ACK is sent to the original station. The address 3 contains the final destination of the frame (in another BSS).

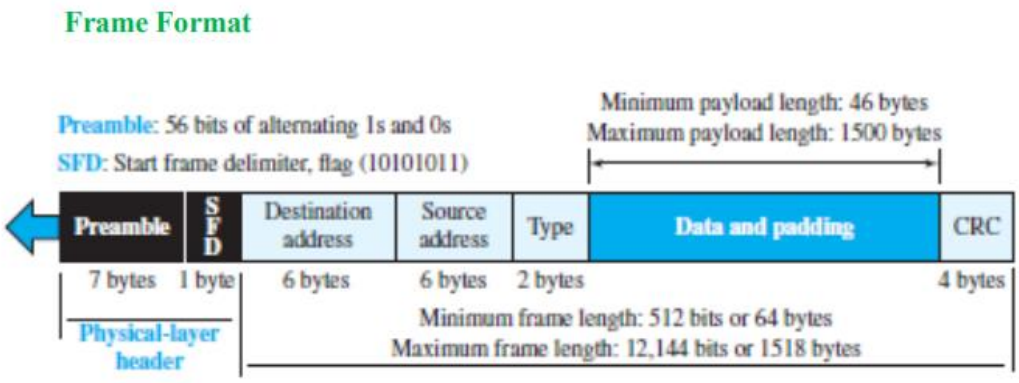
Case-4: 11

In this case, To DS = 1 and From DS = 1 (Figure 15.11d). This is the case in which the distribution-system is also wireless. The frame is going from one AP to another AP in a wireless distribution-system. We do not need to define addresses if the distribution-system is a wired LAN because the frame in these cases has the format of a wired LAN frame (for example: Ethernet,). Here, we need four addresses to define original sender, final destination, and two intermediate APs.

10a)

STANDARD-ETHERNET

The original Ethernet technology with data-rate of 10 Mbps are referred to as the Standard Ethernet. 1. Characteristics Connectionless and Unreliable Service Ethernet provides a connectionless service. Thus, each frame sent is independent of another frame. Ethernet has no connection establishment or connection termination phases. The sender sends a frame whenever it has it. The receiver may or may not be ready for receiving the frame. The sender may overload the receiver with frames, which may result in dropping frames. If a frame drops, the sender will not know about it. If a frame is corrupted during transmission, the receiver drops the frame. Since IP is also connectionless, it will also not know about frame drops. If the transport layer is UDP (connectionless protocol), the frame is lost. If the transport layer is TCP, the sender-TCP does not receive acknowledgment for its segment and sends it again. Ethernet is also unreliable like IP and UDP.

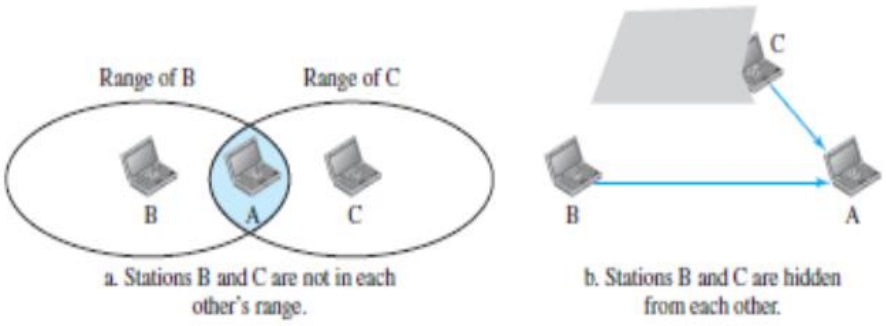


• The Ethernet frame contains 7 fields:
1) Preamble This field contains 7 bytes (56 bits) of alternating 0s and 1s. This field → alerts the receiving-system to the coming frame and → enables the receiving-system to synchronize its input timing. The preamble is actually added at the physical-layer and is not (formally) part of the frame.
2) Start frame delimiter (SFD) This field signals the beginning of the frame. The SFD warns the stations that this is the last chance for synchronization. This field contains the value: 10101011. The last 2 bits (11) alerts the receiver that the next field is the destination-address.
3) Destination-address (DA) This field contains the physical-address of the destination-station.
4) Source-address (SA) This field contains the physical-address of the sender-station.
5) Length or type This field is defined as a i) type field or ii) length field. In original Ethernet, this field is used as the type field. Type field defines the upper-layer protocol using the MAC frame. In IEEE standard, this field is used as the length field. Length field defines the number of bytes in the data-field.
6) Data This field carries data encapsulated from the upper-layer protocols. Minimum data size = 46 bytes. Maximum data size = 1500 bytes.
7) CRC This field contains error detection information such as a CRC-32.

Frame Length
• Ethernet has imposed restrictions on both minimum & maximum lengths of a frame. The minimum length restriction is required for the correct operation of CSMA/CD. Minimum length of frame = 64 bytes. Minimum data size = 46 bytes. Header size + Trailer size = 14 + 4 = 18 bytes. (i.e. 18 bytes 6 bytes source-address + 6 bytes dest-address + 2 bytes length + 4 bytes CRC). The minimum length of data from the upper layer = 46 bytes. If the upper-layer packet is less than 46 bytes, padding is added to make up the difference. Maximum length of frame =1518 bytes. Maximum data size = 1500 bytes. Header size + trailer size = 14 + 4 = 18 bytes. The maximum length restriction has 2 reasons: Memory was very expensive when Ethernet was designed. A maximum length restriction helped to reduce the size of the buffer. This restriction prevents one station from monopolizing the shared medium blocking other stations that have data to send.

10b)
Access Control

The CSMA/CD algorithm does not work in wireless LANs for three reasons: (a) To detect a collision, a host needs to send and receive at the same time which means the host needs to work in a duplex mode. Wireless hosts do not have enough power to do so (the power is supplied by batteries). They can only send or receive at one time. (b) The distance between stations can be great. Signal fading could prevent a station at one end from hearing a collision at other end. (c) Because of the hidden station problem, in which a station may not be aware of another station's transmission due to some obstacles or range problems, collision may occur but not be detected. Hidden station problem Figure 15.3 shows an example of the hidden station problem. Every station in transmission range of Station B can hear any signal transmitted by station B. Every station in transmission range of Station C can hear any signal transmitted by station C. Station C is outside the transmission range of B; Likewise, station B is outside the transmission range of C. However, Station A is in the area covered by both B and C; Therefore, Station A can hear any signal transmitted by B or C.



10c) Fourth Generation (4G)

4G cellular telephony is expected to be a complete evolution in wireless communications. Some objectives defined by the 4G working group: A spectrally efficient system.

High network capacity. Data-rate of 100 Mbps for access in a moving vehicle 1 Gbps for stationary users and 100 Mbps between any two points in the world. Smooth handoff across heterogeneous networks.

Seamless connectivity and global roaming across multiple networks. High quality of service for next generation multimedia support. Interoperability with existing wireless standards. All IP, packetswitched, networks. 4G is only packetbased networks. 4G supports IPv6. 4G provides better multicast, security, and route optimization capabilities.

• Here we discuss, following issues: 1)Access Scheme 2)Modulation 3) Radio System 4)Antenna 5)Applications

1) Access Scheme • To increase efficiency, i) capacity, ii) scalability & iii) new access techniques are being considered for 4G. • For example: i) OFDMA and IFDMA are being considered for the downlink & uplink of the next generation UMTS. ii) MC-CDMA is proposed for the IEEE 802.20 standard.

2) Modulation More efficient 64-QAM is being proposed for use with the LTE standards.

3) Radio System The 4G uses a SDR system. The components of an SDR are pieces of software and thus flexible. The SDR can change its program to shift its frequencies to mitigate frequency interference.
4) Antenna The MIMO and MU-MIMO antenna system is proposed for 4G. Using this antenna, 4G allows independent streams to be transmitted simultaneously from all the antennas to increase the data-rate. MIMO also allows the transmitter and receiver coordinates to move to an open frequency when interference occurs.
5) Applications At the present rates of 15-30 Mbps, 4G is capable of providing users with streaming high definition television. At 100 Mbps, the content of a DVD-5 can be downloaded within about 5 minutes for offline access. (OFDMA Orthogonal FDMA IFDMA interleaved FDMA) (LTE LongTerm Evolution SDR Software Defined Radio) (MIMO multiple-input multiple-output MUMIMO multiuser MIMO) (UMTS Universal Mobile Telecommunications System) (MCCDMA multicarrier code division multiple access)