COMPUTER SCIENCE With python

Textbook for Class XII

- Programming & Computational Thinking
- Computer Networks
- Data Management (SQL, Django)
- Society, Law and Ethics

SUMITA ARORA

DHANPAT RAI & Co.

12 Computer Networks – II

387 – 430

12 Computer Networks – II

In This Chapter

12.1 INTRODUCTION

Computer networks are a result of an efficient collaborative work of some sophisticated hardware and software. Many protocols along with efficiently written software work beautifully along with computers and other network hardware to make 'computer networks' a reality.

This chapter will take you inside the wonderful world of computer networks by discussing various protocols, functioning inside computer networks (modulation techniques, collision detection, error checking, routing, IP addresses) etc., and basic networking tools etc.

12.2 MODULATION TECHNIQUES

You have read that some waves from the *electromagnetic spectrum*, like *radiowaves* and *microwave* etc., are used for carrying data or messages. How these waves carry messages, is the result of a particular technique called **modulation**. Modulation is a process of changing the characteristics of the wave to be transmitted, *i.e.*, **the carrier wave, *by super-imposing the message signal*** on a high-frequency signal.

MODULATION

Modulation is a process of changing the characteristics of the carrier wave by super-imposing the message signal on a high frequency signal.

Modulation Process

A carrier wave by itself doesn't carry much information that we can relate to (such as speech or data). To include *a message* (*i.e., data or speech or image etc.*), another wave, a **message signal** that carries the data to be transmitted, needs to be imposed on top of the carrier signal. This process is termed as **modulation**. Modulation alters the shape of a carrier wave to encode somehow the speech or data information that is to be carried. Now this encoded form of wave (*i.e.*, the speech/data merged with the carrier) will be transmitted. Thus, you can say that modulation is like hiding a code inside the carrier wave. Figure 12.1 shows you the meaning of modulation.

The main function of the carrier wave is to carry the audio or video signal from the transmitter to the receiver. The super-imposition of message signal and carrier wave results into a new wave called the **modulated wave.**

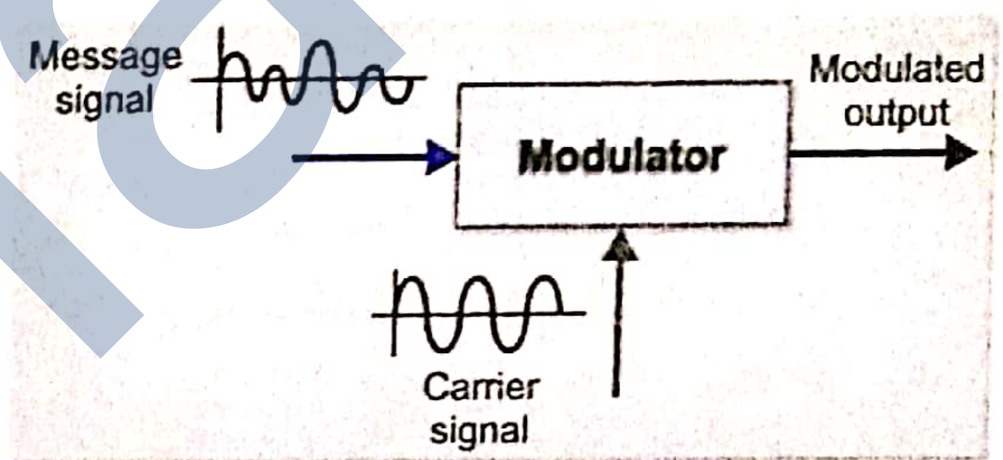
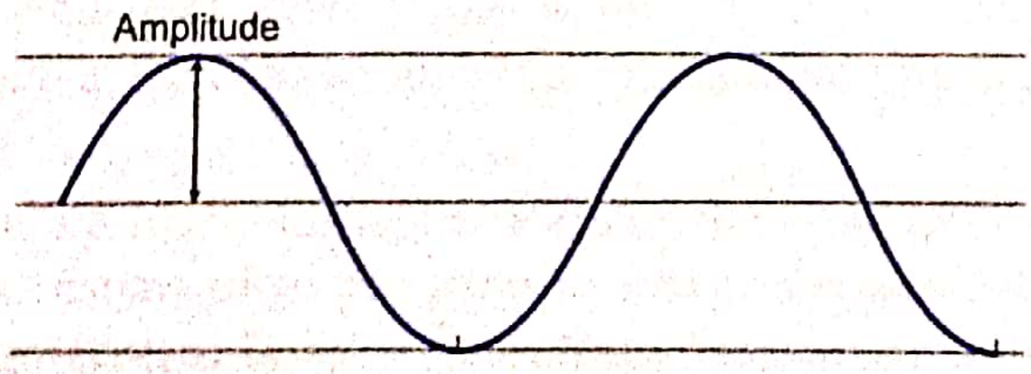


Figure 12.1 Process of modulation.

12.2.1 Major Types of Modulation

Modulation is a technique in which some characteristic of a carrier signal is varied in accordance with a message signal. Two major techniques of modulation work with *two* basic properties of waves : ***amplitude*** and ***frequency***.

- **Amplitude.** The *amplitude* of a wave is its maximum disturbance from its undisturbed position. It is measured in the form of ***the height of the wave***.



- **Frequency.** The *frequency* of a wave is the number of waves produced by a source, per second. It is measured as ***the number of waves that pass a certain point in one second***.

When these two important properties of waves are altered, it results in *two* major types of modulation techniques :

(*i*) Amplitude Modulation (*ii*) Frequency Modulation

12.2.1A Amplitude Modulation (AM)

Let us first try to understand amplitude modulation in simple words. As you know that amplitude is the height of the carrier wave; if, somehow, you can tweak the height of the carrier so that it shows the impact of data/message signal. For example, if an input signal's height varies with the loudness of a user's voice and then adds this to the carrier, then the carrier's amplitude will change corresponding to the input signal that's been fed into it. This is called **amplitude modulation** or **AM**.

AMPLITUDE MODULATION

In **Amplitude Modulation**, the strength of the carrier signal, *i.e.*, the amplitude, is varied as per the changes in the amplitude of the modulating signal.

Following figure (Fig. 12.2) explains the process of amplitude modulation.

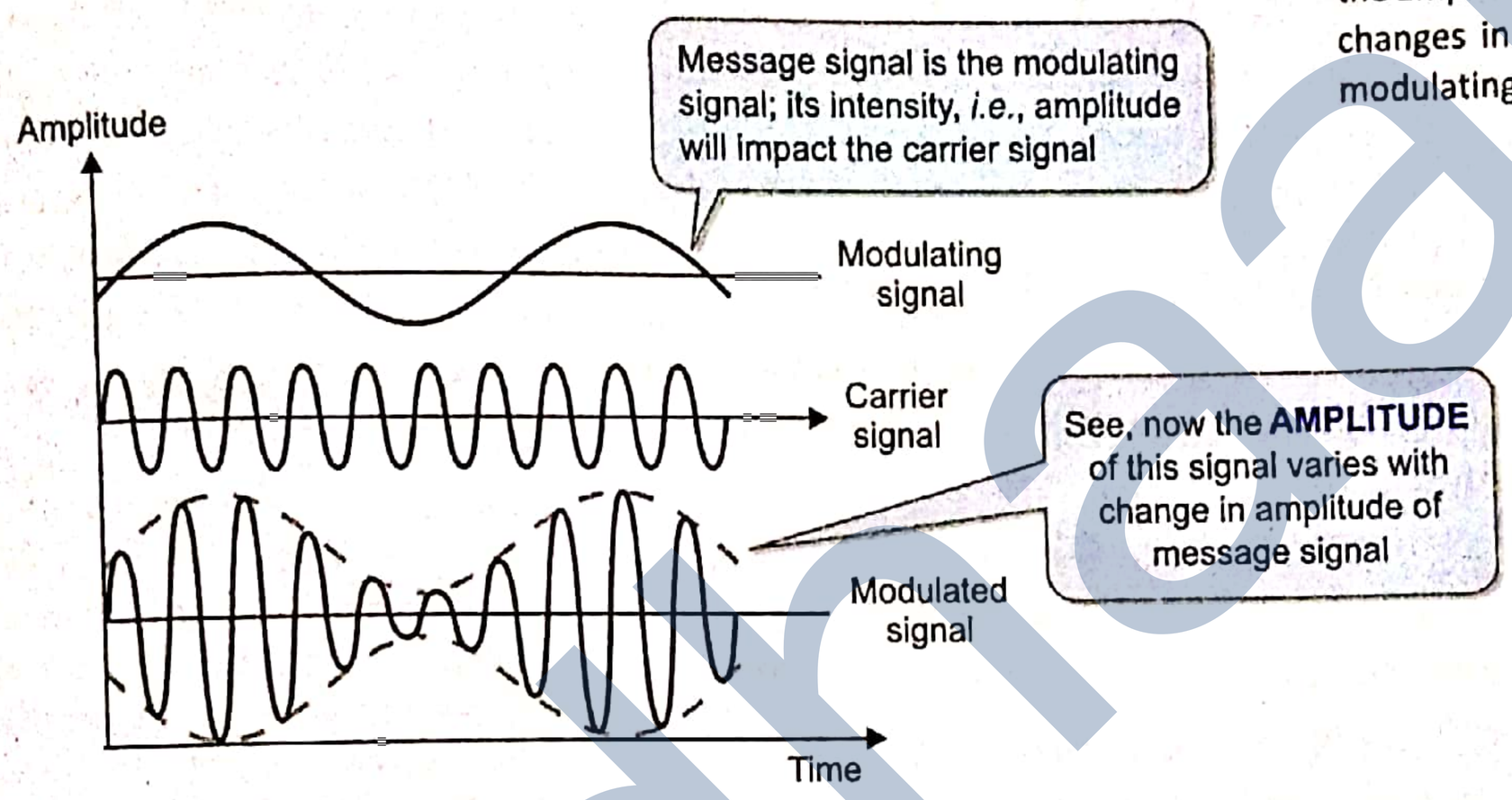


Figure 12.2 Amplitude modulation

So, amplitude modulation is the technique in which the **amplitude of the carrier signal is varied** in line with the variations in the intensity of the *modulating signal*, *i.e.*, the message and the resultant signal is the *modulated signal* (amplitude modulated signal). In this way, the overall amplitude or envelope of the carrier is modulated to carry the actual message. Please note that the other characteristics of the carrier wave (frequency, phase etc.) remain unchanged.

12.2.1B Frequency Modulation (FM)

Just as the amplitude gets varied as per the input message signal in amplitude modulation, the frequency of carrier signal can also be changed as per the input signal. If this input signal is added to the pure carrier wave, it thereby changes the frequency of the carrier wave. In that way, users can use changes of frequency to carry the message information. This is called **frequency modulation** or **FM**.

FREQUENCY MODULATION

In **Frequency Modulation**, the frequency of the carrier signal is varied as per the changes in the amplitude of the modulating signal.

Following figure (Fig. 12.3) explains the process of frequency modulation.

With frequency modulation, the **frequency of the carrier wave is shifted proportionally** to the intensity of the modulating signal. Therefore, the frequency of the modulated wave is shifted continuously. Please note that the other characteristics of the carrier wave (amplitude, phase etc.) remain unchanged.

12.2.1A Amplitude Modulation (AM)

Let us first try to understand amplitude modulation in simple words. As you know that amplitude is the height of the carrier wave; if, somehow, you can tweak the height of the carrier so that it shows the impact of data/message signal. For example, if an input signal's height varies with the loudness of a user's voice and then adds this to the carrier, then the carrier's amplitude will change corresponding to the input signal that's been fed into it. This is called **amplitude modulation** or **AM.**

AMPLITUDE MODULATION

In **Amplitude Modulation**, the strength of the carrier signal, i.e., the amplitude, is varied as per the changes in the amplitude of the modulating signal.

Following figure (Fig. 12.2) explains the process of amplitude modulation.

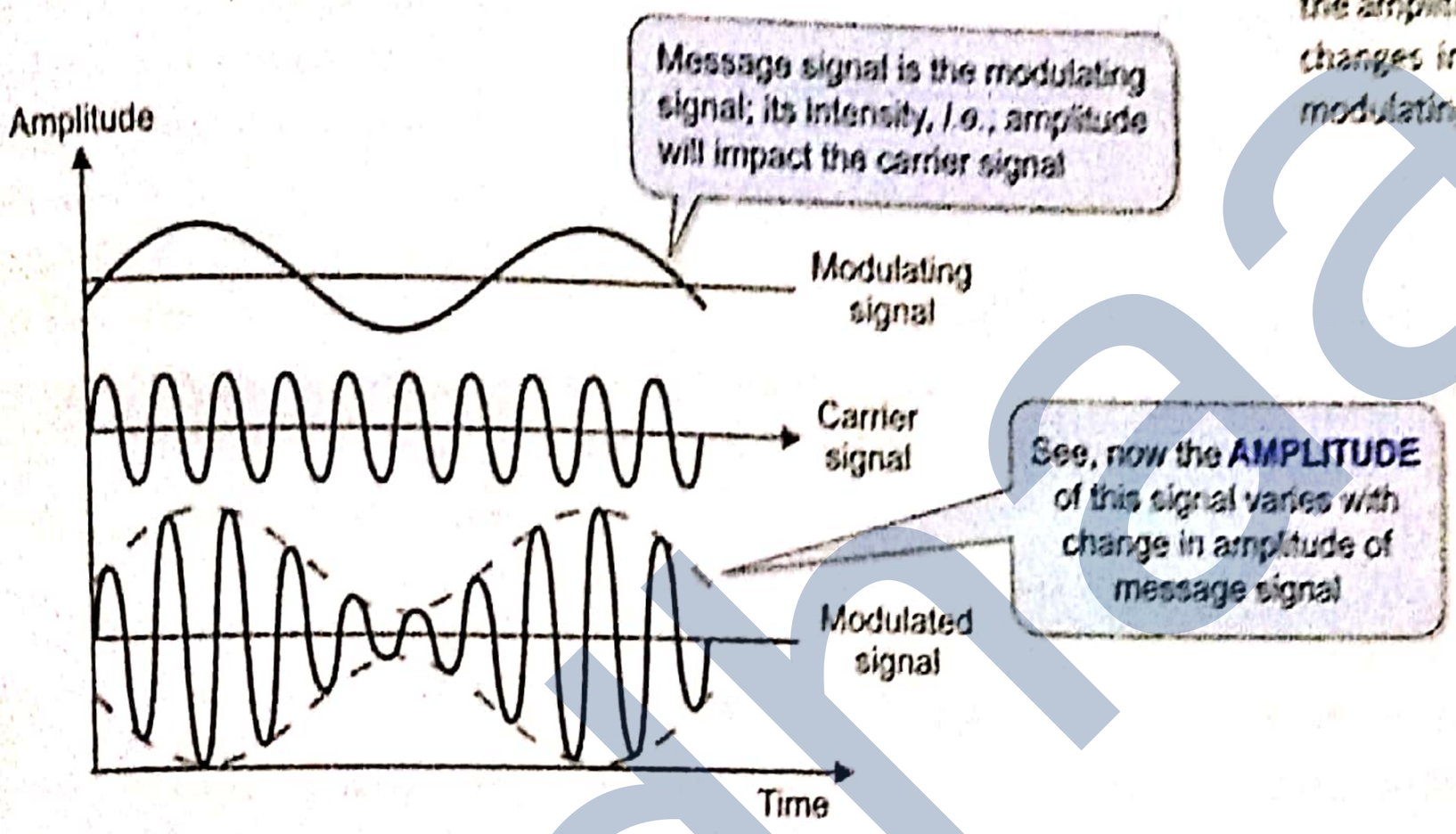


Figure 12.2 Amplitude modulation

So, amplitude modulation is the technique in which the **amplitude of the carrier signal is varied** in line with the variations in the intensity of the *modulating signal*, *i.e.*, the message and the resultant signal is the *modulated signal* (amplitude modulated signal). In this way, the overall amplitude or envelope of the carrier is modulated to carry the actual message. Please note that the other characteristics of the carrier wave (frequency, phase etc.) remain unchanged.

12.2.1B Frequency Modulation (FM)

Just as the amplitude gets varied as per the input message signal in amplitude modulation, the frequency of carrier signal can also be changed as per the input signal. If this input signal is added to the pure carrier wave, it thereby changes the frequency of the carrier wave. In that way, users can use changes of frequency to carry the message information. This is called **frequency modulation** or **FM.**

FREQUENCY MODULATION

In **Frequency Modulation**, the frequency of the carrier signal is varied as per the changes in the amplitude of the modulating signal.

Following figure (Fig. 12.3) explains the process of frequency modulation.

With frequency modulation, the **frequency of the carrier wave is shifted proportionally** to the intensity of the modulating signal. Therefore, the frequency of the modulated wave is shifted continuously. Please note that the other characteristics of the carrier wave (amplitude, phase etc.) remain unchanged.

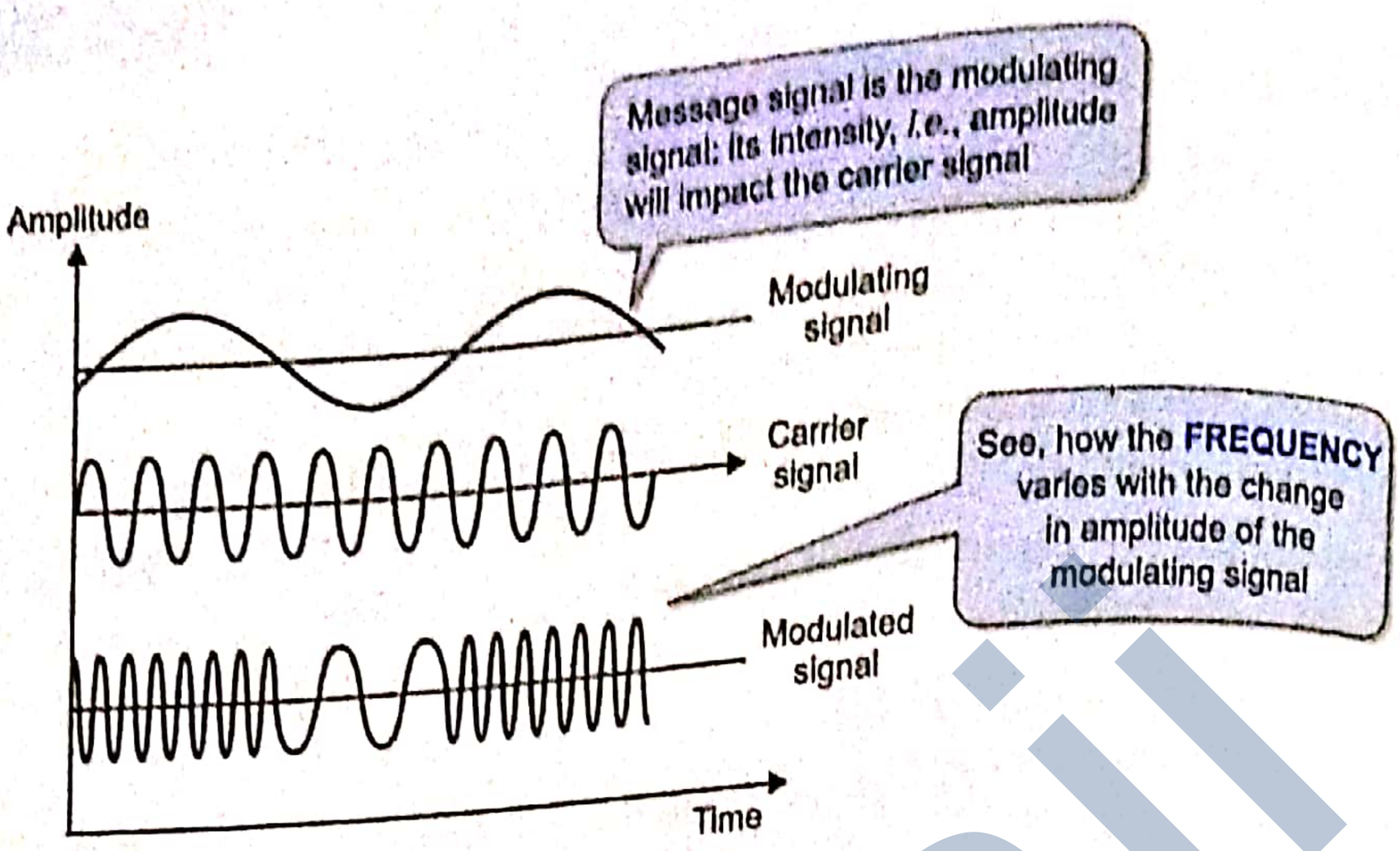


Figure 12.3 Frequency modulation.

As it must be clear to you by now that :

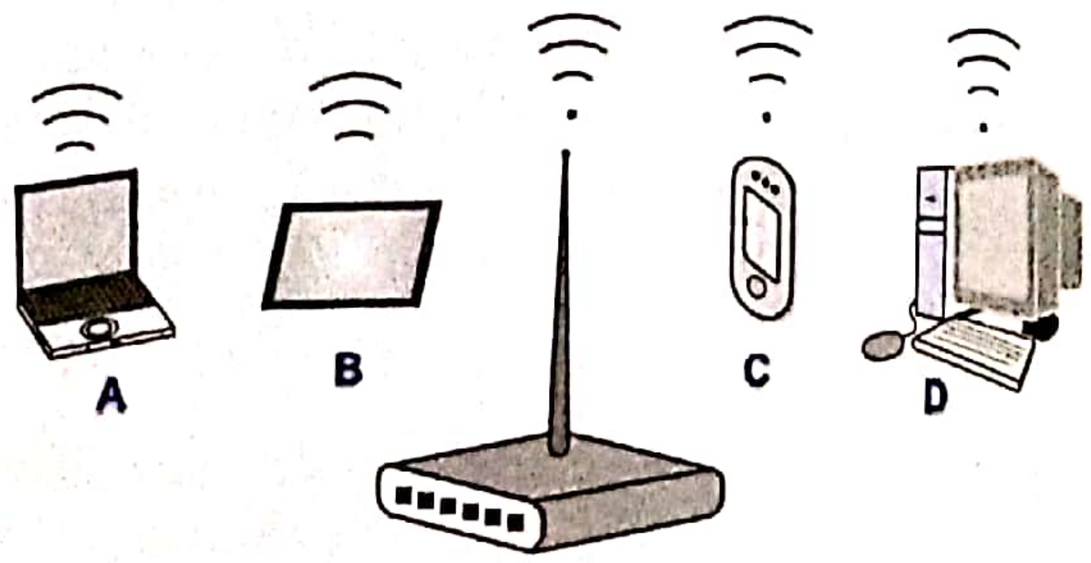
- it is the amplitude of the message signal or the modulating signal that impacts both the modulation techniques.
- if the AMPLITUDE of the carrier wave is varied as per the message signal keeping other characteristics intact, it is the AMPLITUDE MODULATION.
- if the FREQUENCY of the carrier wave is varied as per the message signal keeping other characteristics intact, it is the FREQUENCY MODULATION.

NOTE

Modulation is the technique of changing the characteristics of the signal being transmitted so that it carries data and **Demodulation** is the reverse process of modulation where data is extracted from the received signal (*i.e.*, from the modulated wave).

12.3 COLLISION IN WIRELESS NETWORKS

You know that a wireless network means that its nodes are connected to one another through a wireless communication medium, such as radio-waves. This means that if a wireless network has, say, *four* nodes (*A, B, C* and *D*) then its nodes will communicate to one another using that common, **shared wireless medium** as depicted in the figure here.



COLLISION

In a computer network, **collision** is a specific condition that occurs when two or more nodes on a network transmit data at the same time.

Transmitting over a shared communication medium requires that at a time, only one sender and one receiver use the communication medium. If multiple nodes on the same network transmit data at the same time, it leads to a condition called **collision** and data gets lost. In a computer network, ***collision*** is a specific condition that occurs when two or more nodes on a network transmit data at the same time. Wireless networks use methods to ensure that collisions are avoided. But still, if collision occurs, the nodes wait for a random amount of time and retransmit data packet.

*To understand this concept, imagine when a group of people is conversing. If one person wants to speak and if nobody else is talking, the person simply begins to speak. If someone else is talking, the person waits for him/her to finish. However, it is possible that two people, both noting that nobody is talking, begin to speak at the same time (this is **collision**). They would both realize immediately that they are interfering with each other, would stop talking and wait for a random period before starting again. Eventually, one person would begin speaking again, before the other, and gain the floor.*

In the example above, the two persons who spoke simultaneously were able to detect **collision** as they could speak as well as listen at the same time. Such type of two-way communication where sending and receiving takes place simultaneously, is called **FULL DUPLEX** communication.

But in wireless networks, if collision occurs, the **transmitting nodes cannot detect it**. This is because the nodes in a wireless network cannot listen while transmitting (such type of communication is called **HALF-DUPLEX**). Thus, for wireless networks, strategies are adopted that avoid collision rather than detecting it. Wireless networks implement it using a special protocol (*i.e.*, set of specific rules) called CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance). Wired networks used collision detection methods such as **CSMA/CD (Carrier Sense Multiple Access/Collision Detection)** as wired networks are FULL DUPLEX and hence can receive/listen while transmitting. But CSMA/CD is not suitable for wireless networks, hence CSMA/CA is used for wireless networks.

NOTE

CSMA/CA is used for collision handling in **wireless networks** use a similar mechanism called **CSMA/CD.**

12.3.1 How CSMA/CA Works

The basic working principle of CSMA/CA is described in following lines :

1. Node ready to transmit/talk.
2. Listen for other nodes, if any transmission is taking place. One of the two possibilities are :
   - 2.1 **Busy.** A transmission is taking place. Now do the following :
     - 2.1.1 Increase back off or **wait time** (called BEB (Binary Exponential Backoff))
     - 2.1.2 Sleep as per BEB
     - 2.1.3 Wake up and go to step 1.
   - 2.2 **Free.** No transmission is taking place. Now do the following :
     - 2.2.1 Send Message
     - 2.2.2 Verify it proper transmission has taken place using one of the following two methods :
       - (*a*) ACK (Acknowledgement) Method
       - (*b*) Request to Send/Clear to Send (RTS/CTS) Method

Thus, you can say that there are *two* versions of CSMA/CA :

1. CSMA/CA with ACK (Acknowledgement) method

In this method, as soon as a node transmits data to another node, the receiving node must send an acknowledgement signal called ACK, once it has received the data. The ACK signal must reach to the sender node within a specific time-frame.

If the sender node does not receive ACK in specified time, it considers it as a failed transmission and retransmits the data (*see* Fig. 12.4).

NOTE

The ACK signal is generated by the receiver node, only if the data frame is received in valid form.

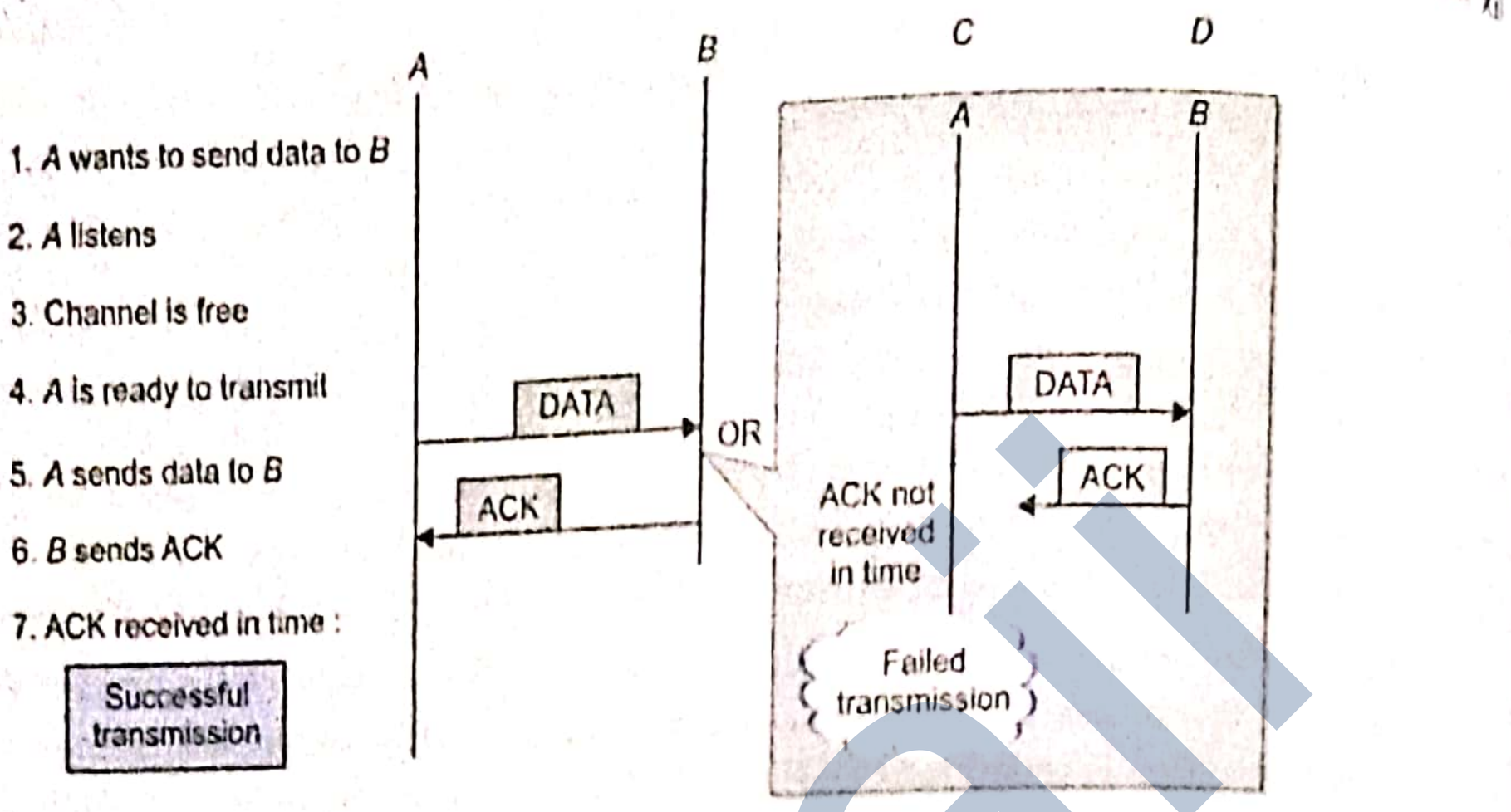


Figure 12.4 CSMA/CA with ACK.

2. CSMA/CA with RTS/CTS (Ready to Send/Clear to Send) method

In this method, the sender node first sends an RTS signal to its receiver. Receiver confirms its readiness to receive by sending a CTS signal to the sender as well as all other nodes.

- Other nodes upon receiving a CTS will now not transmit (will wait) as they now know that some transmission is taking place and communication channel is BUSY.
- The sender node upon receiving a CTS goes ahead with transmission.

Once the transmission ends, the receiver nodes sends ACK signal to all nodes :

- The sender node takes it (ACK) as confirmation of successful transmission.
- Other nodes take ACK signal as end of transmission. Now they can transmit, if they need to as now communication channel is FREE.

NOTE

For smaller wireless networks, **CSMA/CA with ACK** is used, and for bigger wireless networks, **CSMA/CD with RTS/CTS** is used.

Figure 12.5 shows the working of CSMA/CA with RTS/CTS.

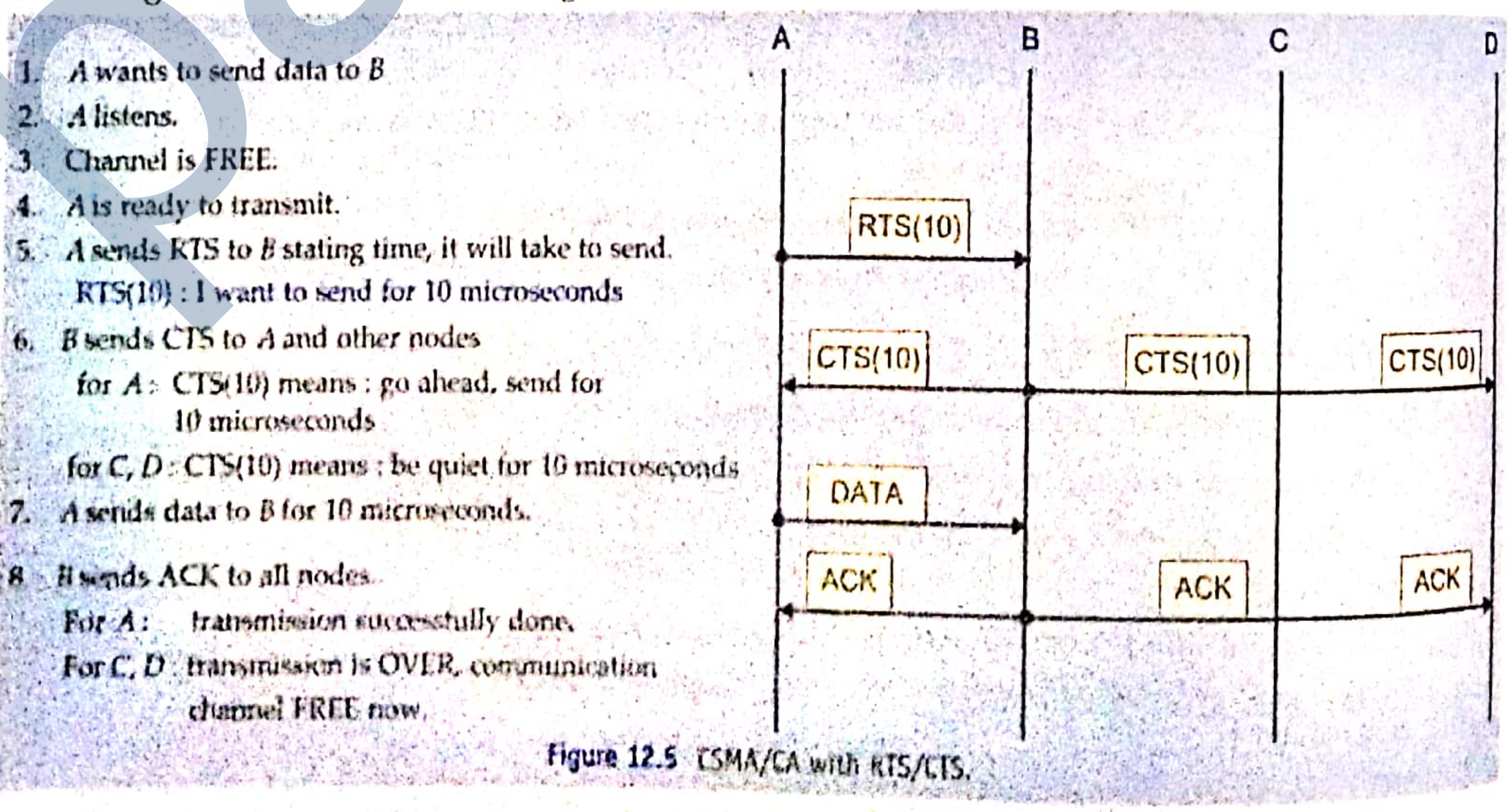


Figure 12.5 CSMA/CA with RTS/CTS.

12.4 ERROR CHECKING (ERROR DETECTION)

While transmitting data over networks, some errors may occur, and data may get corrupted, *e.g.*, if the sender is trying to send a data in binary form as 10110111 and the data received by the receiver as 10110101. If you look carefully, a bit (the 2nd bit from the right) has changed. This means that intended data has not reached the receiver node and hence it is an error.

The errors can be one or more of following types :

(*i*) **Single-bit error.** If only one bit of the transmitted data got changed from 1 to 0 or from 0 to 1.

(*ii*) **Multiple-bit error.** If two or more nonconsecutive bits in data got changed from 0 to 1 or from 1 to 0.

(*iii*) **Burst Error.** If two or more consecutive bits in data got changed from 0 to 1 or from 1 to 0.

To avoid such errors in transmission, some error detection or error checking methods are used in computer networks that ensure if the received packet is error free or not. Here in this section, we are going to talk about some common error checking methods in networks.

1. Single Dimensional Parity Checking

Parity refers to an additional bit added to the actual data. Single dimensional parity check works as described below.

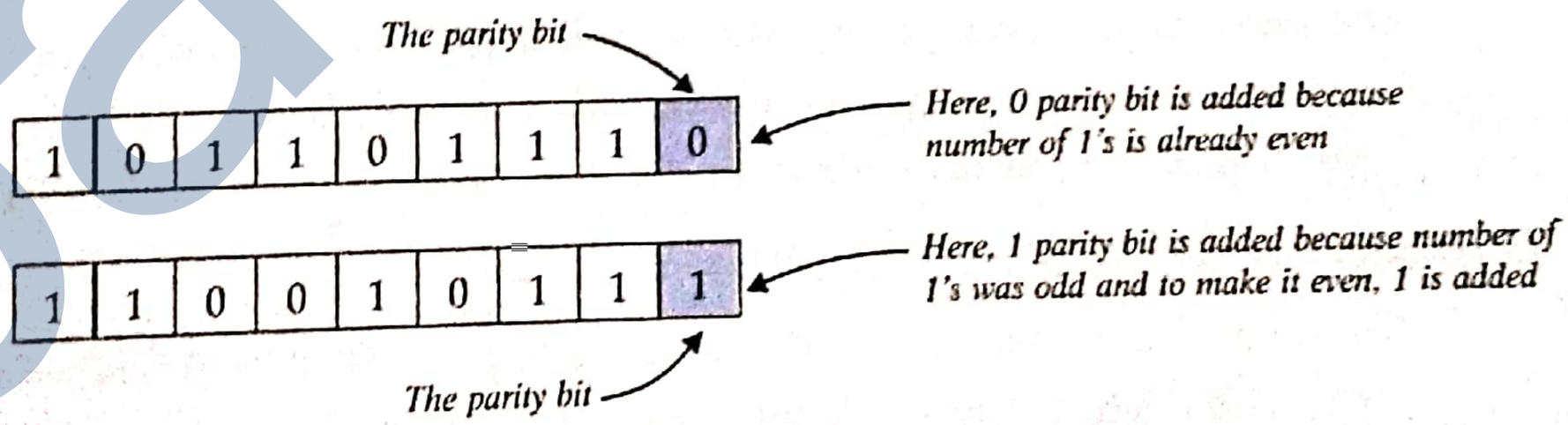
(*For understanding purposes, we are using two sample data units as* ***10110111*** *and* ***11001011.***)

(Before transmission, at the sender node)

(*i*) Number of 1's is counted in the actual data unit.

- In 10110111, the number of 1's is 6, which is an even number.
- In 11001011, the number of 1's is 5, which is an odd number.

(*ii*) Add an extra bit (either 0 or 1), called the **parity bit** to actual data so that the number of 1's along with the extra bit, become even or remain even, *i.e.*, for odd number of 1's, add 1 as the parity bit and for even number of 1's, add 0 as the parity bit.



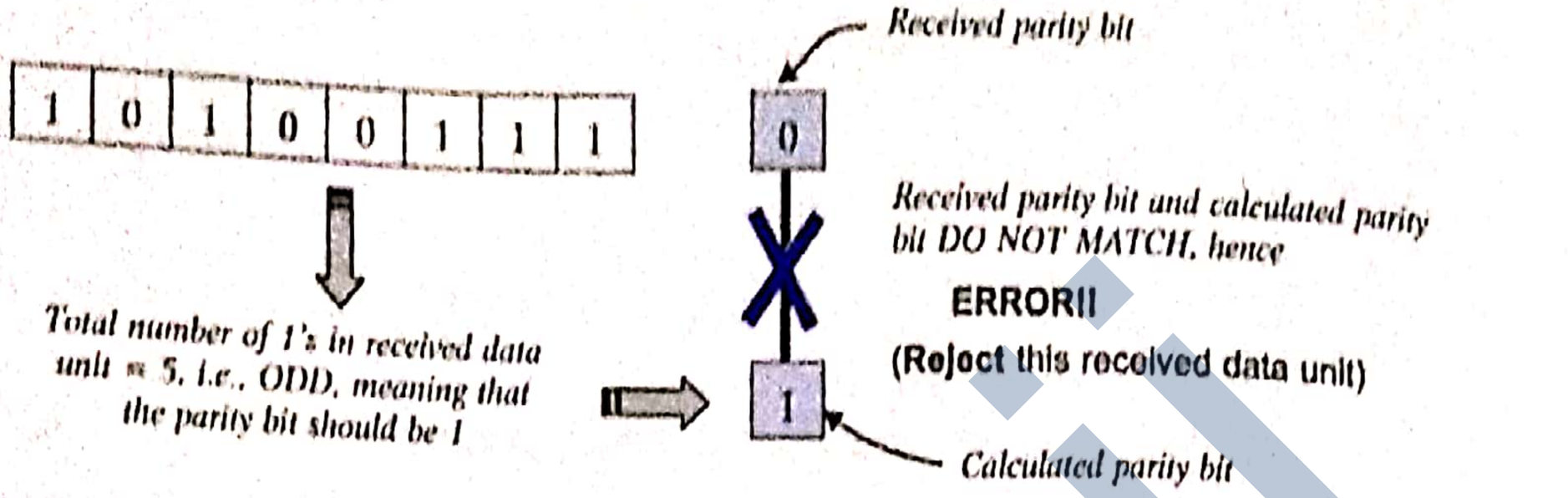
The data is now transmitted along with the parity bit.

(After transmission, at the receiver node)

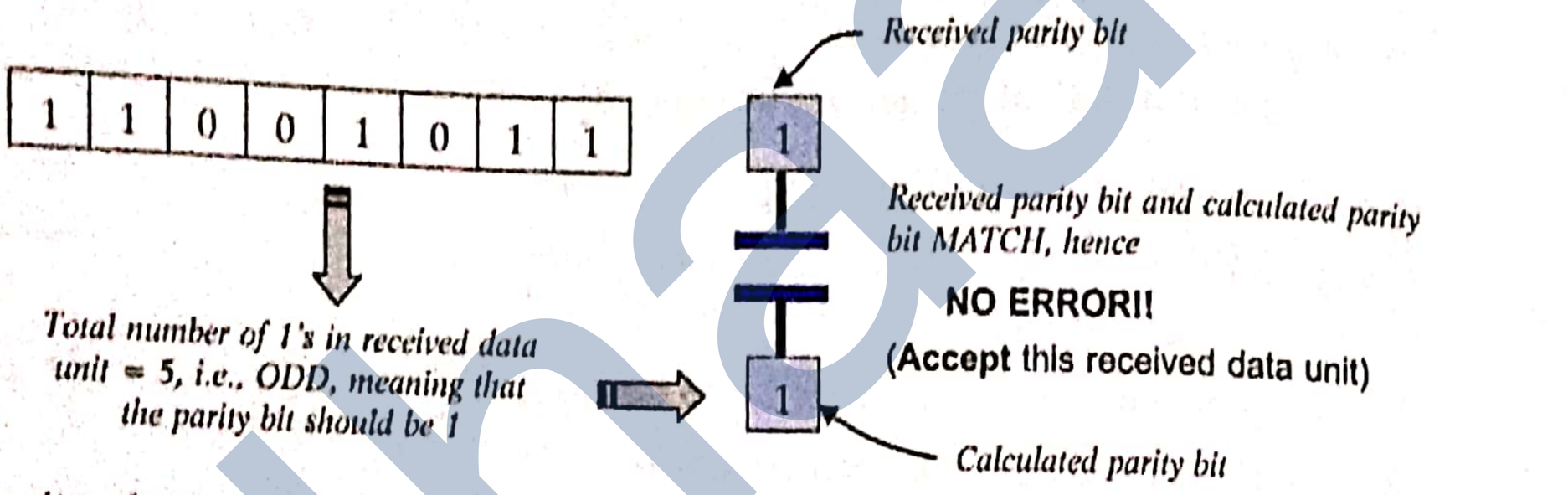
(*iii*) From the received data, excluding the parity bit, **once again determine the parity bit** using the same process, *i.e.*, by calculating the number of 1's in received data and compare it with the received parity bit. If the received parity bit matches with the calculated parity bit, data is considered as CORRECT, otherwise the received data unit is considered as CORRUPTED data and hence rejected[1]. Say, the received data is like **10100111** and **11001011**.

[1] In such a case, the receiver node won't send the ACK signal.

From the received data unit **10100111**, recalculating the parity bit from the data unit part only (excluding the received parity bit) :



Similarly, for other received data unit, *i.e.*, **11001011**, recalculating the parity bit from the data unit part only (excluding the received parity bit) :



Since this parity check is based on making the number of bits as even, it is EVEN PARITY checking. There is ODD parity checking technique also, very similar to this – the only difference is that parity is calculated to make the number of bits ODD.

For Parity Checking technique, the sender and receiver nodes already agree upon which technique (EVEN or ODD parity) will be used for error checking.

Advantages of Single Dimensional Parity Checking

The single dimensional parity checking technique offers following advantages :

(*i*) It is a simple mechanism, which is easy to implements.

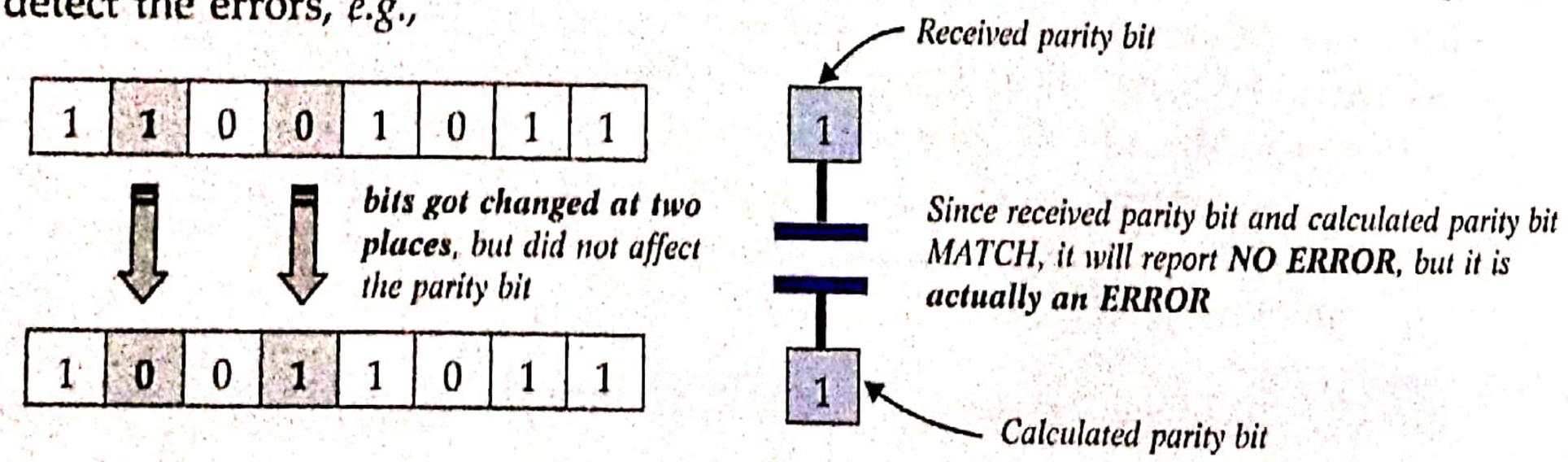
(*ii*) It is an inexpensive technique for detecting the errors in data transmission.

Drawbacks of Single Dimensional Parity Checking

The single dimensional parity checking technique suffers from following drawbacks :

(*i*) It can detect only single-bit errors which occur rarely.

(*ii*) If, in the data transmitted, two bits get interchanged, then even though data gets affected, but the parity bit will remain correct. In such cases, this technique cannot detect the errors, *e.g.*,



2. Two-Dimensional Parity Checking

This is an enhanced version of single dimensional parity checking technique. This technique works with multiple data units simultaneously. This technique works as described below :

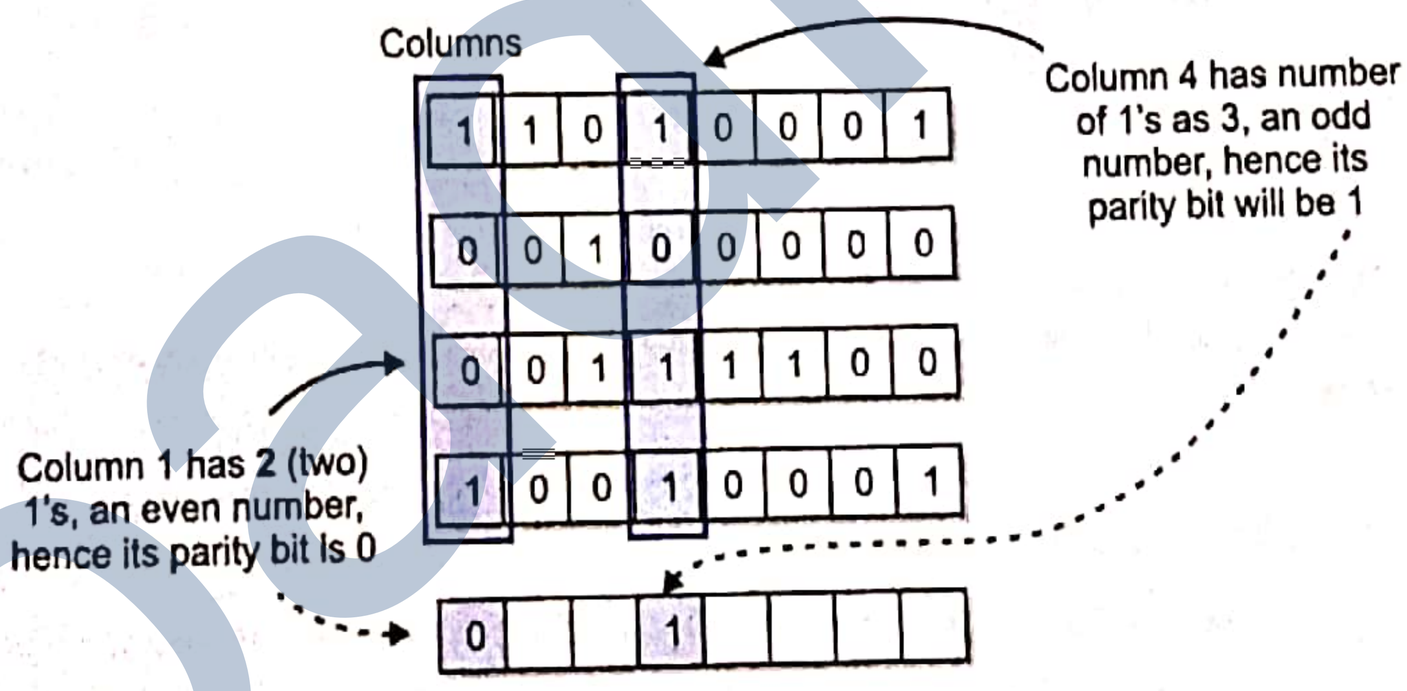
(For understanding purposes, data units being sent are : 11010001, 00100000, 00111100, 10010001)

(At the sender node, before transmission)

(*i*) Organize all data units being sent, one below another so that it appears as table of bits, *i.e.*,

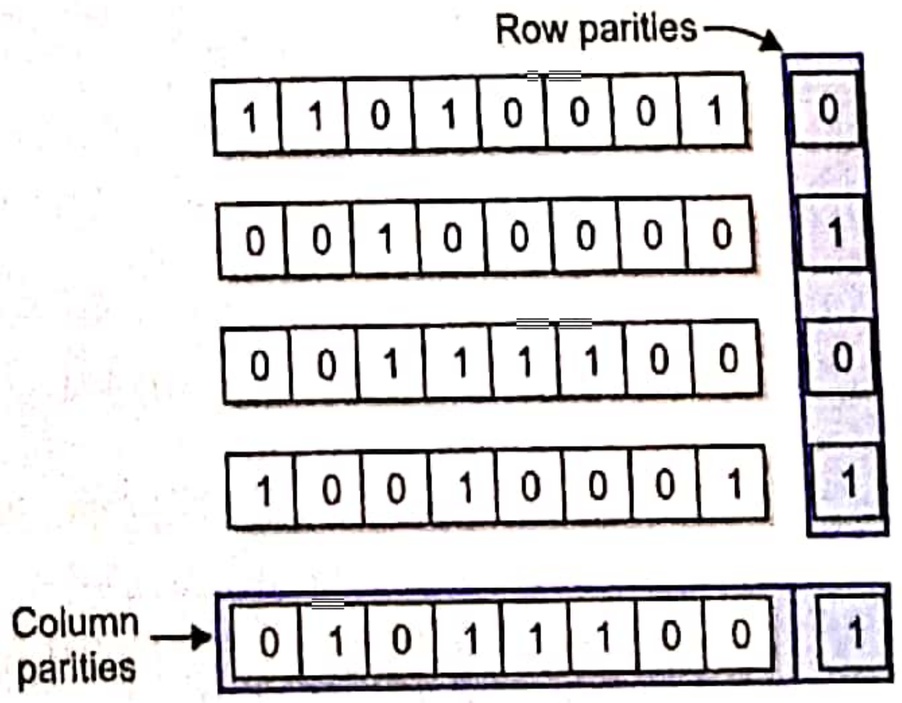
1	1	0	1	0	0	0	1
0	0	1	0	0	0	0	0
0	0	1	1	1	1	0	0
1	0	0	1	0	0	0	1

(*ii*) Calculate parity bits for each data unit row-wise and column-wise. Consider one data unit as a row and bits below one another as columns. Thus, in above data we can say there are four rows and eight columns of bits. That is, calculate column parity as depicted below and row parity in the same manner as you did in **single-dimensional parity check.**



In the same manner, calculate the parity bits for all columns, and also for rows, *i.e.*, two-dimensional parities. So the set of data units along with row parities and column parities will be like as shown here.

The data units are now transmitted with the *row parity bits* and *column parity bits*.

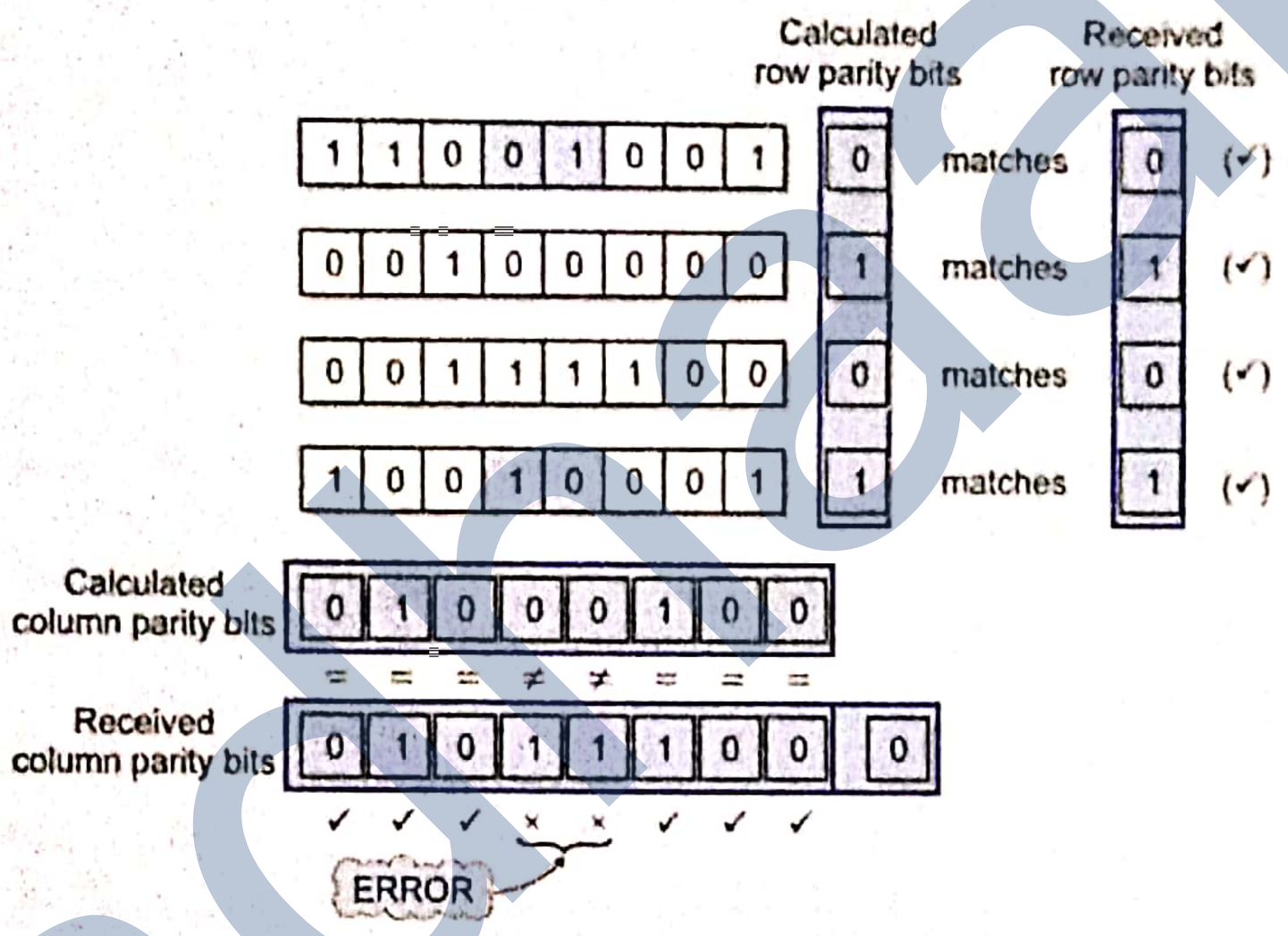


(At the receiver end, after transmission)

(*iii*) The row parity bits and column parity bits are again recalculated using the received data parts only (excluding the parity bits) and compared with the received *row parities* and *column parities*. If these match, data is accepted, otherwise rejected, as this indicates ERROR in transmission.

Say received data units are :

11001001 (*Notice two bits got swapped here*),
00100000, 00111100, 10010001 (*Notice there is error only in first data unit*).



As you can notice that with row parity bits only, errors cannot be detected. However, with two-dimensional parity bits (row parity and column parity), errors can be detected.

Advantages of Two-Dimensional Parity Checking Technique

The two-dimensional parity checking technique offers these advantages :

(*i*) It is more efficient than single dimensional parity technique.

(*ii*) It can detect multiple bit errors also, which sometimes single dimensional parity checking technique cannot.

Drawbacks of Two-Dimensional Parity Checking Technique

The two-dimensional parity checking technique suffers from following drawbacks :

(*i*) It cannot detect compensating multiple bit errors. That means, if two bits in one data unit get corrupted and the two bits at the exact same position in another data unit also get corrupted so that they do not affect row-and column parities, then such an error will go undetected. For example, consider the same example data units as above. If the received data units are as 11001001, 00100000, 00111100, 10001001 – the two bits in first and last data units at exact same positions got corrupted.

									Calculated	Received	
	1	1	0	0	1	0	0	1	0	0	✓ Match
	0	0	1	0	0	0	0	0	1	1	✓ Match
These bits get corrupted but still the error went undetected	0	0	1	1	1	1	0	0	0	0	✓ Match
	1	0	0	0	1	0	0	1	1	1	✓ Match
Calculated	0	1	0	1	1	1	0	0			
Received	0	1	0	1	1	1	0	0			
	✓	✓	✓	✓	✓	✓	✓	✓			

MATCH → NO ERROR
(Errors went unnoticed)

(*ii*) This technique cannot detect 4 – or more–bit errors in some cases.

3. Checksum

The term **checksum** refers to a sum of some bits calculated from digital data that is used to ensure the data integrity at the receiver's end. The checksum is calculated as per a specific scheme and is used for error checking in computer networks. The checksum error detection scheme works as described below :

CHECKSUM

The **checksum** refers to a sum of data bits calculated from digital data that is used to ensure the data integrity at the receiver's end.

(At the sender node, before transmission)

(*i*) The data being transmitted is divided into equal sized k number of segments, where each segment contains m number of bits.

(*ii*) The divided k segments are added using 1's complement arithmetic and extra bits (more than m bits) are added back to the sum (wrap-around).

(*iii*) The final sum's complement is calculated. This is the **checksum**.

(*iv*) Now all the data segments (k segments having m bits each) is sent along with the checksum.

(At the receiver node, after transmission)

(*v*) Step (*ii*) is repeated at the receiver end, *i.e.*, all the data segments are added using 1's complement arithmetic (with extra bits wrapped around) to get the **new sum**.

(*vi*) This **calculated new sum** is added with the **received checksum** and then complemented. Now,

(*a*) if the result is **all 0's**, the transmission is successful (*i.e.*, NO ERROR) – **ACCEPT** the data.

(*b*) if the result is **not all 0's**, the transmission is ERRONEOUS – **REJECT** the data.

In order to calculate checksum practically with some data units, following binary addition rules are used, which state that :

(*a*) 0 + 0 = 0, 0 + 1 = 1, 1 + 0 = 1,
1 + 1 = 11 (where left 1 is a carry bit)

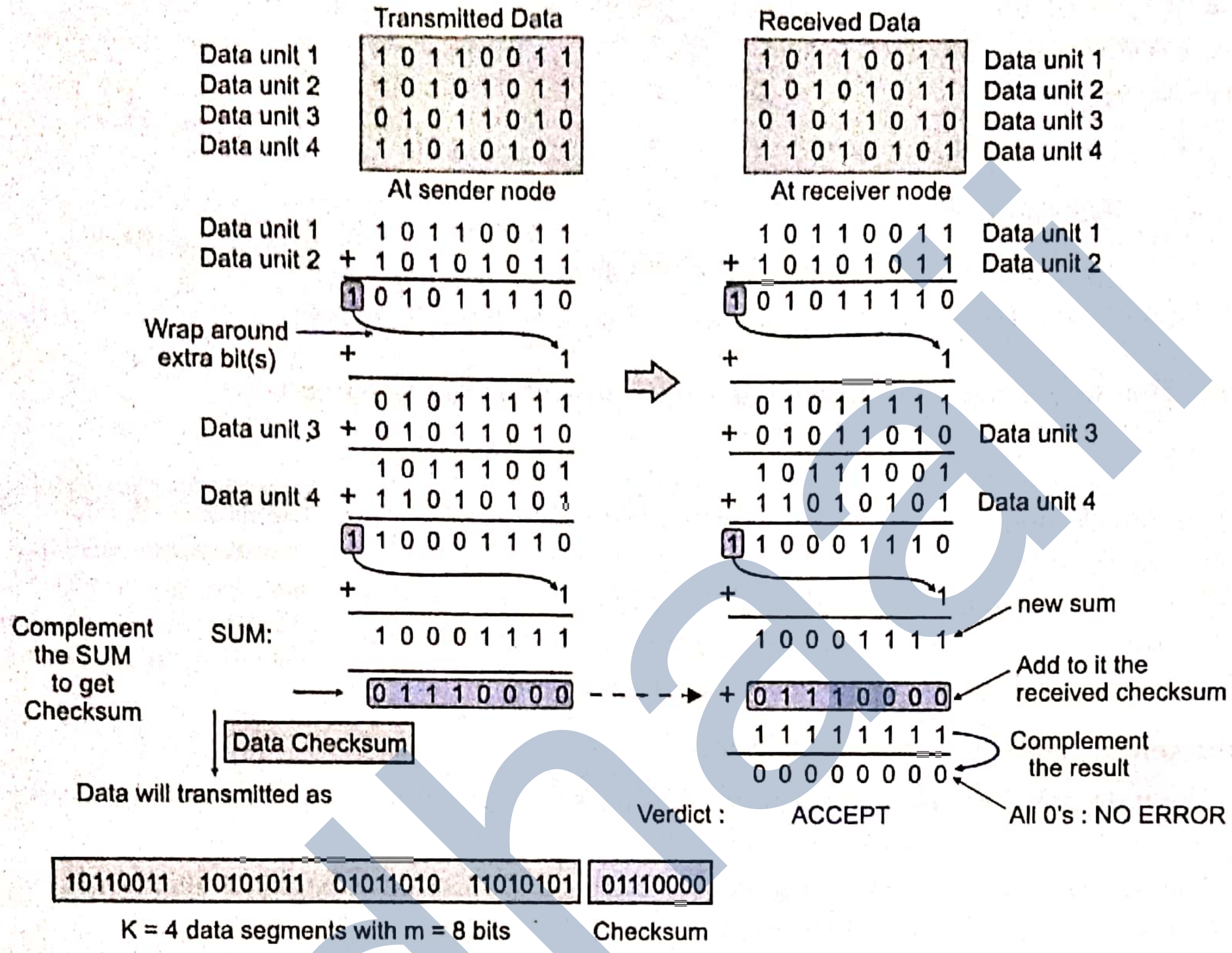
(*b*) Add the last carry bit to the result (wrap-around), *e.g.*,

Carry bits

```
  1 1 1
  1 1 0 1
+ 1 0 1 1
-------
= 1 1 1 0 0
      1
-------
  1 1 0 1
```

Extra bit — *Add this extra bit to the sum, i.e., WRAP-AROUND*

Now let's see how checksum error detection technique works with some data units.



There are many other error checking techniques like CRC (Cyclic Redundancy Check), but we are not covering them here as covering these here, is beyond the scope of this book.

12.5 MAIN IDEA OF ROUTING

You have read about network device **router** in the previous chapter. As routers are responsible for forwarding data in the most efficient way possible, they carry out this job based on many *routing protocols* along with specific *routing information*. The job done by a router is also known as **routing**.

Routing is the process of efficiently selecting a path in a network along which the data packets will travel to their destination. A router maintains a table called **the routing table** that stores routing information based on which the router determines the best path to a network. Routers are not concerned with hosts, they only deal with networks and the best path to reach to them.

Let us quickly have a look at how a router works. There are many different protocols that govern a router's functioning. We shall not goin to details of protocols, rather we shall discuss router's working in simplest way to get the **main idea of routing**.

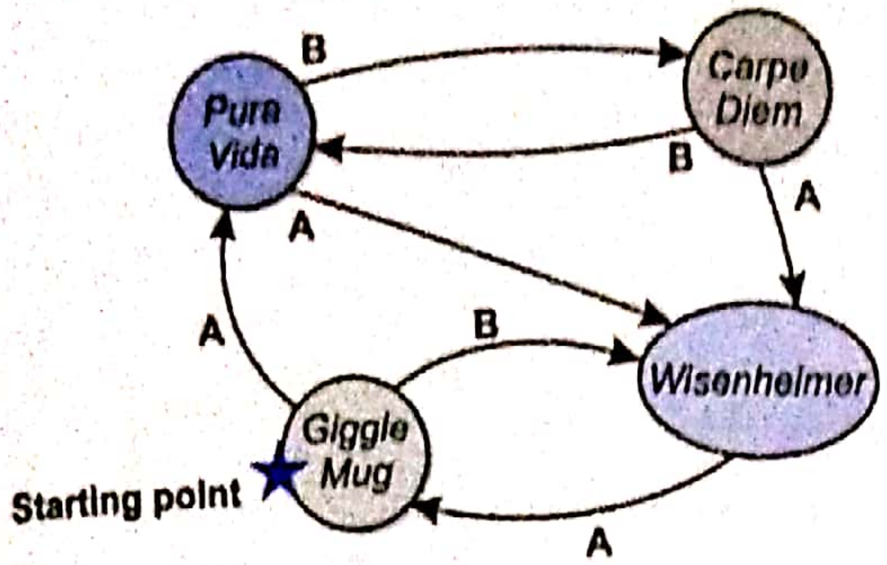
ROUTING

Routing is the process of efficiently selecting a path in a network along which the data packets will travel to their destination.

ROUTING TABLE

A **routing table** is a table maintained by routers that maintains routing information (*i.e.*, about routers to other networks) based on whlch router determines best path to reach to a network.

To understand this, let us recall chapter 11 **'States and Transitions'**, of class XI's book, **'Computer Science with Python'** by *Sumita Arora*. Recall how you determined routers from one island to another. We are listing below the example group of four islands from which you extracted paths as shown below :

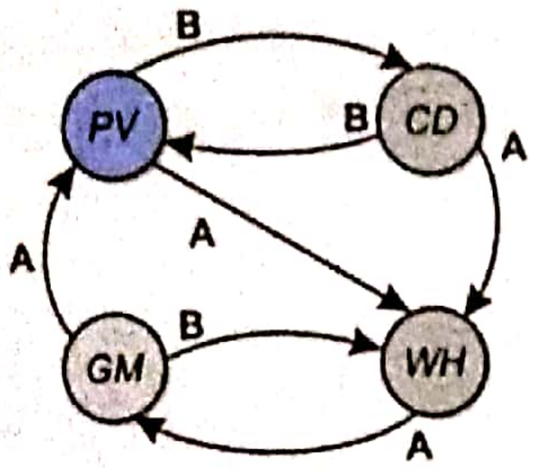


Possible routes from *GiggleMug* island to *Wisenheimer* island are :

B
AA
ABA
BAB
⋮

(*routes from an island as marked as A, B, ...*)

Let us redraw above figure and routes slightly differently as shown below. (We named the islands only by their initial letters.)



From PV to WH

S.No.	Route	Cost
1	B	1
2	AA	2
3	ABA	3
4	BAB	4
⋮	⋮	⋮

Best route is S.No 1 as it costs the least in terms of path travelled.

So, as you can figure out from above table the best path to reach to **WH** from **PV** is route 1 that costs the least of all possible routes.

Now answer me a question – *if, for some reason, route 1 is blocked or cannot be used, what is the next best route to reach to WH from PV* ?

Yes, you guessed it right – **route 2 with cost 2.** (I am so proud of you. ;))

Router also keeps doing something similar. As various networks are connected to one another like a graph (*i.e.*, in the manner similar to the islands), there are multiple paths from one network to another, and router keeps track of best path to reach to another network.

- In fact, router of one network is connected to routers of other networks and they keep exchanging information such as which networks they can reach etc.
- Every router maintains a table called **routing table** that stores the best paths to reach to other networks starting from it.
- Routers work with one goal : **Find the best route for every destination.**

Let us now understand *routing* with the help of following example where routers of different networks are connected as shown here.

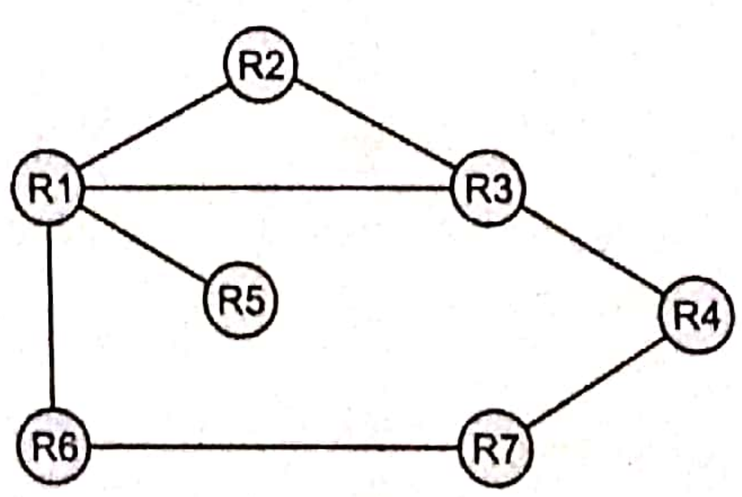


Figure 12.6

Router R2's routing table will store the best routes for all other routers, along with the *next hop* that will determine which route to take.

R2's Routing Table :

Destination	Cost	Next Hop
R1	1	R1
R3	1	R3
R4	2	R3
R5	2	R1
R6	2	R1
R7	3	R1

e.g., this row means that from R2 to R6 the cost is 2 via router R1, and this is the best route so far.

- Now if a request asks R2 to send data to **R4**, then it checks its routing table and finds that the best route to reach **R4** is **via R3**. So **R2** will forward the data packet to router **R3** along with the intended destination.

  R3 upon receiving the data packet (intended for **R4**) will check its own routing table (R3's routing table) and send to the router on the best path for **R4** (which is **R4** itself.)

  This way, the data packet will reach to its destination.

How router updates its routes in case of problems like link broken or increased network traffic ?

Let us now see how a router adapts to changes in network. Following lines will illustrate how a router does this. Before that remember that :

- Every router maintains its ***routing table*** storing details of the best routes originating from it to all other networks.
- Every router keeps sending its updated routing tables (R.T.) to all the routers directly connected to it – periodically and also in case of a problem.
- Based on received updates, a router keeps updating its R.T. to store the information about the best routes.
- At time T_0, 3 routing tables (R.T.) belonging to **R6**, **R1** and **R3** (as per Fig. 12.6) are :

R6's R.T. (at Time T_0)

Dest.	Cost	Next
R1	1	R1
R2	2	R1
R3	2	R1
R4	3	R1
R5	2	R1
R7	1	R7

R1's R.T. (at Time T_0)

Dest.	Cost	Next
R2	1	R2
R3	1	R3
R4	2	R3
R5	1	R5
R6	1	R6
R7	2	R6

R3's R.T. (at Time T_0)

Dest.	Cost	Next
R1	1	R1
R2	1	R2
R4	1	R4
R5	2	R1
R6	2	R1
R7	2	R4

- At Time T_1, R6 detects that link to R7 has failed. So R7 sets cost to reach R7 as infinity (∞) and updates its R.T. and sends update to R1.

R6's R.T. (Time T_1)

Dest.	Cost	Next
⋮	⋮	⋮
⋮	⋮	⋮
~~R7~~	~~1~~	~~R7~~
R7	∞	R7

- At Time T_2, R1 receives update from R6 and accordingly updates its own R.T. as it uses **R6** to reach R7 (last entry of its table)

R1's R.T. (Time T_2)

Dest.	Cost	Next
⋮	⋮	⋮
⋮	⋮	⋮
~~R7~~	~~2~~	~~R6~~
R7	∞	R6

- At Time T_3, R1 receives periodic update from R3 that says that R3 can reach R7 with a cost of 2 hops. Thus, based on this, R1 updates its R.T. and sets costs of reaching R7 via R3 as 3 (one extra hop to reach to R3 and then 2 hops from R3).

  Upon updating its routing table, it sends updates to all its connected routers including **R6**.

R1's R.T. (Time T_3)

Dest.	Cost	Next
⋮	⋮	⋮
⋮	⋮	⋮
~~R7~~	~~2~~	~~R6~~
~~R7~~	~~∞~~	~~R6~~
R7	3	R3

- At Time T_4, R6 receives this update from R1 and finds out that it can reach R7 via R1 by adding cost by 1 hop (additional hop from R6 to R1)

R6's R.T. (Time T_4)

Dest.	Cost	Next
⋮	⋮	⋮
⋮	⋮	⋮
~~R7~~	~~1~~	~~R7~~
~~R7~~	~~∞~~	~~R7~~
R7	4	R1

This is the processing of routing, which keeps updating the routing table (R.T.) of a router. Whenever, a router receives a data packet to be sent to a network, the router will look for the best path to reach to that network's router and send data pack to the router mentioned as **next hop** for that.

12.6 TCP/IP

The TCP/IP suite is the current de facto standard for both local and wide area networking. TCP/IP is used as the primary or sole communication protocol on nearly all new computer network installations.

Currently, the Internet fully supports TCP/IP version 4 (*IPv4*). Internet has started adapting to TCP/IP version 6 (*IPv6*). TCP/IP is not tied to any one vendor, and therefore allows heterogeneous networks to communicate efficiently.

TCP/IP is a collection of protocols that includes *Transmission Control Protocol, Internet Protocol, User Datagram Protocol (UDP)* and many others. Each of these protocols has a specific function :

TCP TCP ensures reliable communication and uses ports to deliver packets. It is a **connection-oriented protocol.** TCP also fragments and reassembles messages, using a sequencing function to ensure that packets are reassembled in the correct order. In TCP, a connection must be built using a *handshake process* before information is sent or received. A *handshake process* means establishing a direct connection between sender and receiver with start signal, acknowledgement signals etc.

UDP UDP is a **connectionless protocol**. It allows information to be sent without using a handshake process. It is often used to transfer relatively small amounts of information.

IP IP is a **connectionless protocol** responsible for providing addresses of each computer and performing routing.

12.6.1 Network Congestion and Retransmission in TCP

Network congestion is a special situation in a computer network where the network devices such as routers have to deal with much more data incoming to them than they can handle at a time. Network congestion results in many problems such as :

(*i*) The receiving network device (such as *router*) cannot send acknowledgment signal (ACK signal) in time even if they have received the data correctly.

(*ii*) The sender node retransmits the data when it does not receive the ACK signal and, this further increases the network traffic, **causing more congestion.**

(*iii*) It **reduces the network throughput.** Throughput is a measure of a network's performance.

NETWORK CONGESTION

Network congestion is a specific condition in a network when more data packets are coming to network devices than they can handle and process at a time.

Symptoms of Network Congestion

Networks identify the congestion situation through the following symptoms :

(*i*) excessive packet delay (*ii*) loss of data packets (*iii*) retransmission.

How Network Congestion is Handled ? (Analogy to Road Network Congestion)

Network congestion is analogous to the congestion on roads and can be handled similarly. To control the roads' congestion problem, often a technique called **metering** is used that controls the incoming traffic (or the number of vehicles entering a road) on roads by employing measures like ***traffic-signals*** or ***rerouting the traffic.***

The **metering** technique is implemented to control network congestion, in the following way :

(*i*) It ensures that the sender does not overflow the network and it is done by *controlling the flow of data packets* (**rate modulation of data packets**). With this measure, the sender maintains a value indicating the limit of data that can be sent into the network without being acknowledged.

(*ii*) It ensures that the routers along the path work as per their capacity to handle network traffic and do not become overflowed. It includes strategies like :

(*a*) rerouting the data packets.

(*b*) informing the senders about the congestion to control the transmission rate.

(*c*) delaying the transmission/retransmission depending upon the congestion levels.

12.7 ADDRESSES ON A NETWORK

On a network, various types of addresses play roles. Different addresses used on a network are :

(*a*) Web Address (URL) (*b*) IP Address

Web Address (URL)

A location on a net server is called a web site. Each web site has a unique address called **URL** (Uniform Resource Locator) *e.g.*, the web site of Microsoft has an address or URL called **http://www.microsoft.com.**

Let us explore it further. The Internet structure of the World Wide Web is built on a set of rules called **Hypertext Transfer Protocol (HTTP)** and a page description language called **Hypertext Markup Language (HTML)** generally. HTTP uses Internet addresses in a special format called a **Uniform Resource Locator** or **URL.**

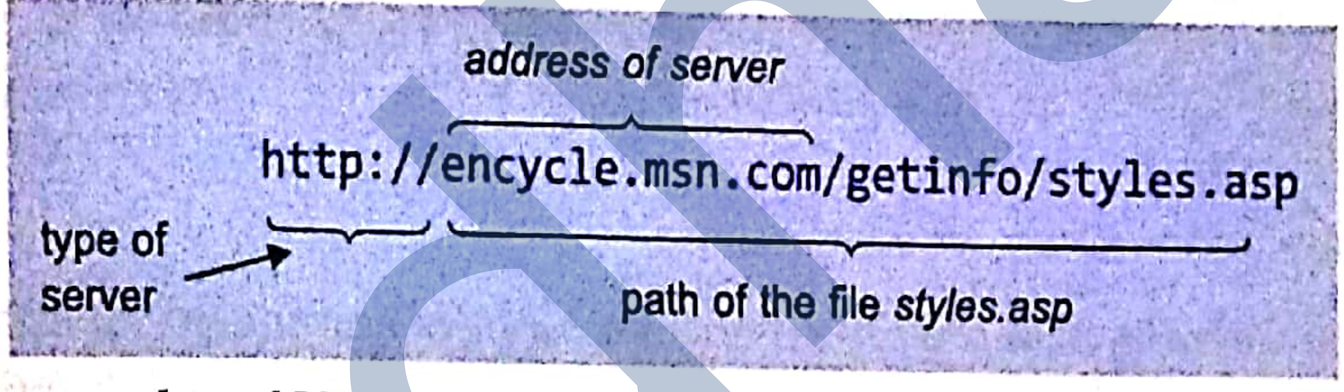
URL

A location on a net server is called a URL (Uniform Resource Locator).

URLs look like this :

```
type://address/path
```

where *type*: specifies the type of server in which the file is located, *address* is the address of server, and *path* tells the location of file on the server. For example, in the following URL



The other examples of URLs are

`ftp://ftp.prenhall.com`, `http://www.yahoo.com`, `news://alt.tennis` etc.

A URL is also referred to as *Web Address* sometimes.

Elements of a URL

A URL (Uniform Resource Locator) is an address of a file on Internet. Let us discuss the components or syntax elements of URLs.

A file's Internet address, or URL, is determined by the following :

- The type of server or protocol
- The name/address of the server on the Internet
- The location of the file on the server (this location may be related as a "path" through the file hierarchy)

NOTE

The characters based naming system by which servers are identified is also known as domain name system (DNS).

Table 12.1 lists the types of servers you may encounter, along with the protocol they use, and the type(s) of information they provide.

In any typical URL *e.g.*, **http://www.khoj.com**, the "http" identifies both the protocol and server. (According to standard URL syntax, a colon (:) and two forward slashes (//) follow the protocol/server.)

Similarly, in URL ftp://www.mypubserver.com, the "ftp" identifies both the protocol and server. Here it is *FTP* type of server. Refer to table 12.1 for more types of servers.

Table 12.1 Internet Servers and What they Provide

Server	Protocol	Information It Provides
ftp	File Transfer Protocol	Text and binary files that are organized in a hierarchical structure, much like a family tree.
gopher	Transfer Control Protocol/Internet Protocol (TCP/IP)	Text and binary files that are organized in a menu structure.
http	Hypertext Transfer Protocol	Hypertext/hypermedia files (*i.e.*, multimedia documents that contain links to images, sounds, or other multimedia documents on the World Wide Web).

The next component of the address is the name of the server, in this case, **www.khoj.com.** Server names have multiple components. Commonly (but not always) a Web server's name will begin "www" for World Wide Web. The ".com" suffix (called a ***domain* indicator**) indicates that Khoj is a commercial entity, as opposed to a nonprofit organization (".org"), a school or university (".edu"), a branch of the government (".gov"), etc. The naming scheme by which servers are identified is also known as the *domain name system*.

IP Address

IP ADDRESS

IP address is a unique numerical label as a string of numbers separated by dots, used to identify a device on the internet.

Each network device (a computer or any other network device) on a TCP/IP network needs to have a unique address on the network. This unique address on a TCP/IP network is the IP Address. *IP addresses are needed so that different networks can communicate with each other.*

IP addresses can be thought of as a unique series of numbers, uniquely identifying a computer on a network. Thus, you can say that just like, telephones are uniquely identified through their telephone-numbers, computers on a TCP/IP network (such as Internet) are uniquely identified through their unique addresses – *IP addresses*.

Each IP address is actually a series containing four numbers separated by dots or periods *e.g.*, *192.168.1.1* is an IP address. Similarly, *10.217.1.1* is also an IP address and so on.

IP addresses are normally written in ***dotted decimal form*** as listed above but computers internally convert them into ***binary form***.

For instance,

```
an IP address in dotted decimal form : 216.27.61.137
same IP address in binary form : 11011000.00011011.00111101.10001001
```

Internet Protocol Versions

There are currently *two* versions of Internet Protocol (IP). **IPv4** and a newer version called IPv6. IPv6 is an evolutionary upgrade to the Internet Protocol. IPv6 will coexist with the older IPv4 for some time.

(*i*) **IPv4** is the most widely deployed Internet protocol used to connect devices to the Internet. IPv4 uses a 32-bit address scheme allowing for a total of 2^{32} addresses (just over 4 billion addresses). With the growth of the Internet it is expected that the number of unused IPv4 addresses will eventually run out because every device — including computers, smartphones and game consoles — that connects to the Internet requires an address.

(*ii*) A new Internet addressing system Internet Protocol version 6 (**IPv6**) is being deployed to fulfill the need for more Internet addresses. IPv6 utilizes 128-bit Internet addresses. Therefore, it can support 2^{128} Internet addresses —

340,282,366,920,938,000,000,000,000,000,000,000,000 of them to be exact.

In other words, there are more than enough IPv6 addresses to keep the Internet operational for a very, very long time.

IPv4 vs. IPv6 Addresses

IPv4 addresses are **32 bits** long while **IPv6** addresses are **128 bits long**. Other than the size, there are other differences in these two TCP/IP internet addresses. Let us learn how IPv4 and IPv6 Internet addresses are different from one another.

NOTE

The IP addresses are very important as these are needed by network devices to reach to a specific computing device.

(A) IPv4 Address

An IPv4 address has the following format : **x . x . x . x**, where **x** is called an **octet** and must be a **decimal value** between 0 and 255. Octets are separated by periods. An IPv4 address must contain ***three periods and four octets.***

The following examples are valid IPv4 addresses as shown on the right.

Since, there are 4 octets in an *IPv4* address, the total possible combinations of unique *IPv4* addresses are 4, 294, 967, 296.

```
1.2.3.4
01.102.103.104
19.117.63.126
198.162.1.1
```

IPv4 addresses :
4 octets separated by periods(dots)

(B) IPv6 Address

An IPv6 address can have either of the following *two* formats :

(*i*) **Normal.** Pure IPv6 format (*ii*) **Dual.** IPv6 plus IPv4 formats

(*i*) ***Normal IPv6 Address.*** An IPv6 (Normal) address has the following format :

y : y : y : y : y : y : y : y

where **y** is called a segment and can be any **hexadecimal value** between **0** and **FFFF**. The segments are **separated by colons** - not periods. An IPv6 normal address must have **eight segments** ; however, at some places zero segments can also be omitted.

The following list shows examples of valid IPv6 (Normal) addresses :

```
2001 : db8: 3333 : 4444 : 5555 : 6666 : 7777 : 8888
2001 : db8 : 3333 : 4444 : CCCC : DDDD : EEEE : FFFF
: :                  (implies all 8 segments are zero)
2001: db8: :         (implies that the last six segments are zero)
: : 1234 : 5678      (implies that the first six segments are zero)
2001 : db8: : 1234 : 5678    (implies that the middle four segments are zero)
2001:0db8:0001:0000:0000:0ab9:C0A8:0102
                     (This can be compressed to eliminate
                     leading zeros, as follows: 2001:db8:1::ab9:C0A8:102 )
```

IPv6 addresses :
8 segments separated by colons

(*ii*) ***IPv6 (Dual) Address.*** An IPv6 (Dual) address combines an IPv6 and an IPv4 address and has the following format :

y : y : y : y : y : y : x . x . x . x

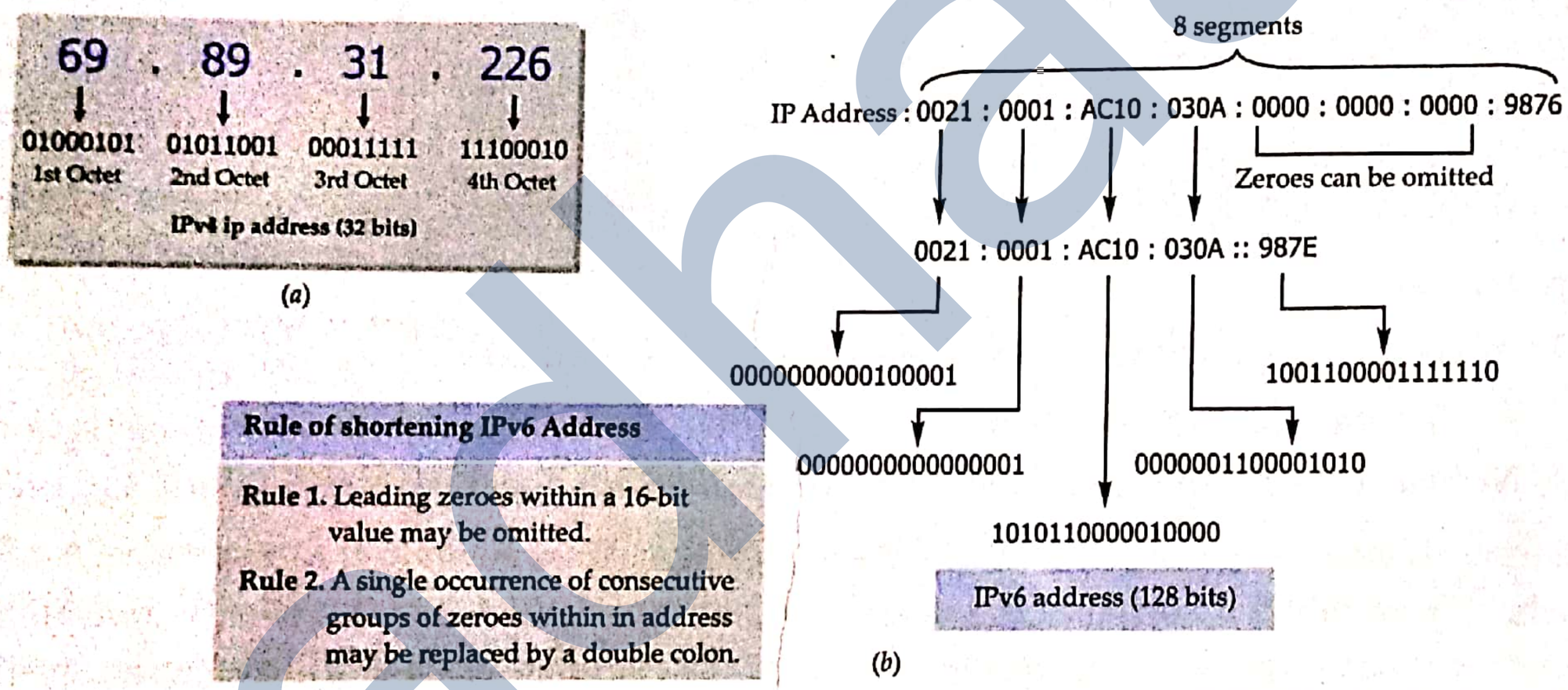
The IPv6 portion of the address (indicated with y's) is always at the beginning, followed by the IPv4 portion (indicated with x's).

In the IPv6 portion of the address, y is called a ***segment*** and can be any hexadecimal value between 0 and FFFF. The segments are *separated by colons - not periods*. The IPv6 portion of the address must have ***six segments*** but there is a short form notation for segments that are zero.

In the IPv4 portion of the address x is called an **octet** and must be a decimal value between 0 and 255. The octets are separated by periods. The IPv4 portion of the address must contain *three periods and four octets*. The following list shows examples of valid IPv6 (Dual) addresses :

```
2001 : db8 : 3333 : 4444 : 5555 : 6666 : 1 . 2 . 3 . 4
: : 11 . 22 . 33 . 44                    (implies all six IPv6 segments are zero)
2001 : db8: : 123 . 123 . 123 . 123      (implies that the last four IPv6 segments are zero)
: : 1234 : 5678 : 91 . 123 . 4 . 56      (implies that the first four IPv6 segments are zero)
: : 1234 : 5678 : 1 . 2 . 3 . 4          (implies that the first four IPv6 segments are zero)
2001 : db8: : 1234 : 5678 : 5 . 6 . 7 . 8
                                         (implies that the middle two IPv6 segments are zero)
```

Figure 12.7 shows the difference between IPv4 and IPv6 Internet addresses.



Rule of shortening IPv6 Address

Rule 1. Leading zeroes within a 16-bit value may be omitted.

Rule 2. A single occurrence of consecutive groups of zeroes within in address may be replaced by a double colon.

Figure 12.7 (*a*) IPv4 Internet address (*b*) IPv6 Internet address.

12.7.1 The Domain Name and DNS

The URL of a website is also known as its **domain name**. The domain name is unique name of a website. A domain name generally contains following parts :

(*i*) www[2]

(*ii*) name describing the website's purpose

(*iii*) TLD (Top Level Domain) such as .com, .net, .org, .edu, .ca, .in, .jp etc.

Examples of some domain names are :

www.amazon.com ; www.wayn.com.cn ; www.mybiz.co.in ; www.dce.edu ; www.cbse.nic.in

DOMAIN NAME

The **Domain Name** is a unique name assigned to a website.

NOTE

All domain names are URLs but not vice-versa *e.g.*, **www.edupillar.com** is a domain name and a URL too but the URL www.edupillar.com/about us/ is a URL, not a domain name.

2. **There can be exceptions too, *e.g.*, msn.com (without www).**

12.7.1A Domain Name Resolution (DNS)

In a previous section, we discussed that all computers connected in a TCP/IP networks have IP addresses and in order to reach to any computer, its IP address is required.

As you know that the websites are mostly accessed through their *domain names*, because the *domain name* is much easier to memorise and recognize.

Since a website is hosted on a computer and in order to reach to a website, its host computer must be reached. Therefore, the IP address of the computer is required.

NOTE

A domain name is also known as DNS name i.e., Domain Name System name.

Now what is the way out ? You know the domain name of the computer and not its IP address, but its IP address is needed in order to reach there. The wayout is *Domain Name Resolution*, which in simple words means – the process of finding corresponding IP address from a domain name.

NOTE

Domain Name Resolution refers to the process of obtaining corresponding IP address from a *domain name*.

How Domain Name Resolution Works

The domain name resolution takes place behind the scene and you as a user would not be able to notice it. Let's see what all happens behind the scenes in domain name resolution.

(*i*) You enter the domain name in an application (say a web-browser) in order to reach there.

(*ii*) The application, where the domain name has been typed (Web Browser in our case), now issues a command to operating system asking it to provide the corresponding IP address of the given domain name.

(*iii*) Now operating system tries to resolve the domain name as per its configuration (different OSs such as Windows, Linux, Unix etc. are configured differently).

Mostly the operating systems resolve it as depicted below :

(*a*) *Refer to its HOSTS file to obtain corresponding IP address.* Most operating systems maintain a HOSTS file that stores IP addresses of some domains. Therefore, first of all, OS looks into this file to obtain corresponding IP address, if it is listed there.

(*b*) If the previous method fails, then operating system connects to a **DNS (Domain Name System) Server** on Internet. The DNS servers on Internet maintain directory of IP addresses of all domain names registered on Internet. The DNS servers work out to obtain corresponding IP address of given domain name and return it to operating system.

(*iv*) After obtaining IP address of given domain name, the operating system passes this information to the application (browser in our case) that demanded it.

12.8 CELLULAR/WIRELESS CONNECTIVITY PROTOCOLS

Modern age cellular or wireless networks depend heavily on wireless connectivity protocols such as 2G, 3G, 4G etc.

2G GSM (1992) – the Second Generation

2G, more familiarly known as GSM was introduced back in 1992 and is a fully digital technology. It allowed some data along with calls in the form of text messages. GSM can handle **data speeds of up to 250 Kbps.**

The GSM standard is transmitted at **frequencies between 900 Mhz and 1800 Mhz.**

3G (2000) – the Third Generation Standard

3G was introduced to cater to increasing demand for data by consumers. 3G initially offered speeds of 500 Kbps to 2 Mbps, but over the years, it is now as high as 20 Mbps! It can handle data in the form of text messages and multimedia such as audio/video messages along with voice calls.

3G is transmitted at frequency 2100 Mhz.

4G (2013) – the Fourth Generation

4G offers data speeds in the range of 10 – 15 Mbps, which can go up to 50 Mbps and even higher depending on the technology. The operators use many different frequencies for 4G. In India the frequency range for 4G (LTE) is 1800 Hz to 2300 Hz.

What makes a protocol have a higher bandwidth?

In networking, bandwidth refers to the transmission capacity of a computer or a communications channel. It is stated in megabits per second (Mbps).

Higher frequencies offer higher bandwidth. It means they can handle more users, more data at the same time. And by transmitting at both high and low frequencies (800 Mhz and 2600 Mhz), they can get the 4G signal to propagate into the countryside and also offer the high bandwidth to city users.

Wi-Fi

Wi-Fi (Wireless Fidely) protocol governs the rules to connect to the Internet without a direct line from your PC to the ISP. For Wi-Fi to work, you need:

- A broadband Internet connection.
- A wireless router, which relays your Internet connection from the "wall" (the ISP) to the PC.
- A laptop or desktop with a wireless internet card or external wireless adapter.

Wi-Fi Hotspots. A hotspot is a venue that offers Wi-Fi access. The public can use a laptop, WiFi phone, or other suitable portable device to access the Internet through a WiFi Hotspot.

12.9 BASIC NETWORK TOOLS

When you are connected to Internet, you might encounter many problems. To figure out what type of errors are obstructing your connection, you may need to work with different network tools or simple networking commands.

In order to use these commands. You have to type them in front of command prompt. In Linux, you do this on a terminal. In Windows, you need to run **cmd** application first. To run **cmd** on a Windows computer, just type **cmd** in the search box (available from start button) and click the **cmd** application name it shows. Now on the prompt in **cmd window**, you can issue these commands.

We are going to discuss basic network tools basic networking commands below.

12.9.1 PING

To test the connectivity between two hosts, you can use the PING command. PING determines whether the remote machine (website, server, etc.) can receive the test packet and reply. It is determined by finding how much time it takes to get the response from the remote machine.

Ping serves *two* purposes :

1. To ensure that a network connection can be established.
2. Timing information as to the speed of the connection.

NOTE

Ping command will work when you are connected to Internet.

You can use *ping* as per following format :

ping <domain name or ip address>

```
C:\Users\Edup>ping cbseacademic.nic.in

Pinging cbseacademic.nic.in [164.100.230.217] with 32 bytes of data:
Reply from 164.100.230.217: bytes=32 time=24ms TTL=116
Reply from 164.100.230.217: bytes=32 time=19ms TTL=116
Reply from 164.100.230.217: bytes=32 time=35ms TTL=116
Reply from 164.100.230.217: bytes=32 time=22ms TTL=116

Ping statistics for 164.100.230.217:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 19ms, Maximum = 35ms, Average = 25ms
```

12.9.2 TRACEROUTE (for Linux) or TRACERT (for Windows)

To trace the network path, the signal takes from your computer to the destination computer (whose domain name is given with the command), you can use TRACEROUTE command. **Traceroute** or **Tracert** is very similar to **Ping**, except that it identifies which network pathways it takes along each hop, rather than the time it takes for each packet to return.

NOTE

Traceroute is a handy utility to view the number of hops and response time to get to a remote system or website. Like ping, for traceroute too, you need an internet connection to make it work.

You can use this command as per following format :

Tracerout or tracert <domain name or ipaddress>

```
C:\Users\Edup>tracert cbseacademic.nic.in

Tracing route to cbseacademic.nic.in [164.100.230.217]
over a maximum of 30 hops:

  1     2 ms     3 ms     2 ms  192.168.0.1
  2    29 ms    12 ms    13 ms  10.225.0.1
  3    15 ms    11 ms    11 ms  202.88.149.145
  4    12 ms    21 ms    15 ms  202.88.149.66
  5     *        *        *     Request timed out.
  6     *        *        *     Request timed out.
  7     *        *        *     Request timed out.
  8     *        *        *     Request timed out.
  9     *        *        *     Request timed out.
 10     *        *        *     Request timed out.
 11     *        *        *     Request timed out.
 12     *        *        *     Request timed out.
 13     *        *        *     Request timed out.
 14    19 ms    18 ms    18 ms  164.100.230.217

Trace complete.
```

12.9.3 NSLOOKUP

For diagnosing DNS name resolution problems, you can use the command **NSLOOKUP**. When you type **NSLOOKUP** in front of the command prompt, it does two things :

(*i*) It displays the name and IP address of your computer's default DNS server.

(*ii*) It also displays a small prompt that is nslookup's own prompt. Here you can type the domain name or IP address. The result determines if your DNS server can resolve the given domain or IP address.

```
C:\Users\Edup>nslookup
Default Server:  delhi-dns.hathway.com
Address:  202.88.149.25

>
```

Domain name and ipaddress of your computer's default DNS server

Nslookup's own prompt. Type here domain name or ipaddress

(see examples on next page)

Some sample domain names and ipaddreses resolved via *nslookup command* are shown below.

```
C:\Users\Edup>nslookup
Default Server:  delhi-dns.hathway.com
Address:  202.88.149.25

> cbseacademic.nic.in
Server:  delhi-dns.hathway.com
Address:  202.88.149.25

Non-authoritative answer:
Name:    in.domain.name
Address:  185.82.212.199
Aliases:  cbseacademic.nic.in.domain.name

> 115.72.192.15
Server:  delhi-dns.hathway.com
Address:  202.88.149.25

Name:    adsl.viettel.vn
Address:  115.72.192.15

>
```

Press CTRL+C to end nslookup's interactive mode

Press CTRL+C to end nslookup's interactive mode.

12.9.4 IPCONFIG Command

The IPCONFIG command displays detailed information about the network you are connected to. It is used as per following formats :

`ipconfig` or `ipconfig/all`

The **ipconfig/all** command gives more detailed information such as DNS servers, DHCP enabled or not, MAC Address, along with other helpful information.

```
C:\Users\Edup>ipconfig

Windows IP Configuration

Wireless LAN adapter Wireless Network Connection 2:

   Connection-specific DNS Suffix  . : domain.name
   Link-local IPv6 Address . . . . . : fe80::c0b:92f:361e:3071%19
   IPv4 Address. . . . . . . . . . . : 192.168.0.3
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::1e5f:2bff:fe4f:b1f%19
                                       192.168.0.1
```

```
C:\Users\Edup>ipconfig/all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : Edup-PC
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : domain.name

Wireless LAN adapter Wireless Network Connection 2:

   Connection-specific DNS Suffix  . : domain.name
   Description . . . . . . . . . . . : D-Link DWA-131 Wireless N Nano USB Adapte
r(rev.E)
   Physical Address. . . . . . . . . : 40-9B-CD-97-83-82
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::c0b:92f:361e:3071%19(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.0.3(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Friday, January 18, 2019 12:57:09 PM
   Lease Expires . . . . . . . . . . : Friday, January 18, 2019 3:57:09 PM
   Default Gateway . . . . . . . . . : fe80::1e5f:2bff:fe4f:b1f%19
                                       192.168.0.1
   DHCP Server . . . . . . . . . . . : 192.168.0.1
   DHCPv6 IAID . . . . . . . . . . . : 339778509
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-1F-3C-7C-71-BC-AE-C5-8F-43-93

   DNS Servers . . . . . . . . . . . : 202.88.149.25
                                       202.88.149.6
                                       202.88.131.91
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

12.9.5 WHOIS Command

WHOIS is a query command that is used to get some information on a specific domain name, such as who registered it, when was it registered, and when the domain will expire etc. This command is used as per format :

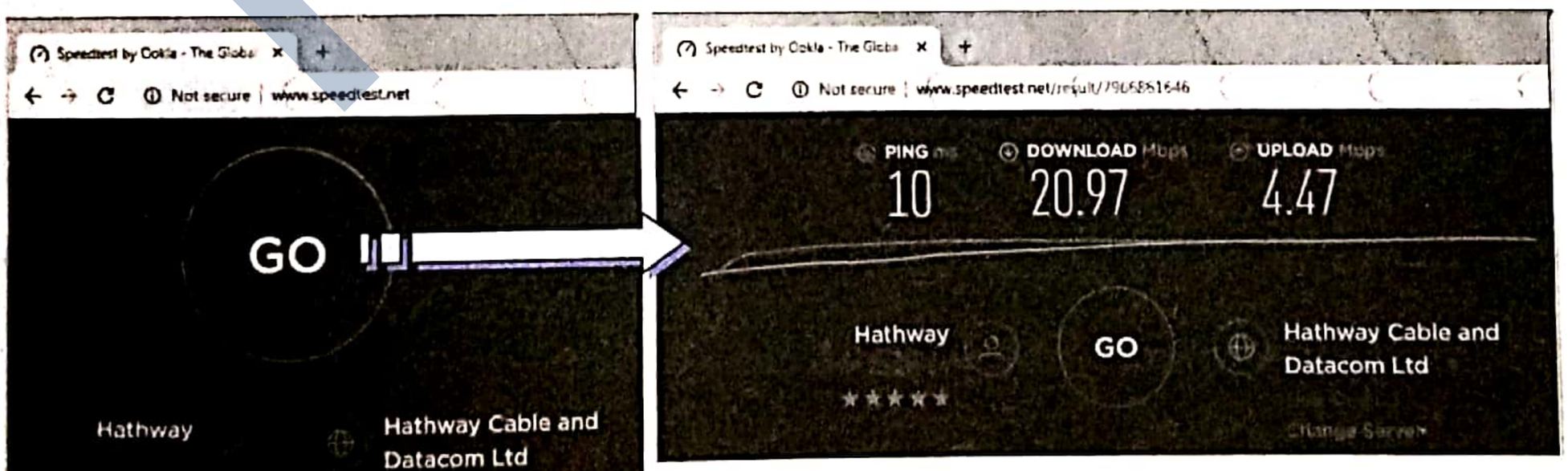
```
whois -h <domain name>
```

```
C:\Users\Edup>whois -H google.com

Whois Server Version 2.0

Domain names in the .com and .net domains can now be registered
with many different competing registrars. Go to http://www.internic.net
for detailed information.

   Domain Name: GOOGLE.COM
   Registrar: MARKMONITOR INC.
   Sponsoring Registrar IANA ID: 292
   Whois Server: whois.markmonitor.com
   Referral URL: http://www.markmonitor.com
   Name Server: NS1.GOOGLE.COM
   Name Server: NS2.GOOGLE.COM
   Name Server: NS3.GOOGLE.COM
   Name Server: NS4.GOOGLE.COM
   Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
   Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
   Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
   Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
   Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
   Updated Date: 20-jul-2011
   Creation Date: 15-sep-1997
   Expiration Date: 14-sep-2020
```

12.9.6 Speed Test

To check the download and upload speeds of your network connections, you can use a speed-test utility. There are many speed-test utilities available online, but we shall use the site speedtest.net's utility for this.

To check the speed of your network, go to site **speedtest.net** while you are online and then click GO. You may need to choose your server also. It will then show you download and upload speeds of your network at that point of time.



12.10 VARIOUS PROTOCOLS USED ON NETWORKS

A protocol refers to a set of rules. Networking happens when two or more different computers connect and interact with one another and share data in many ways. For interactions, some agreed up rules called protocols are used by the interacting parties. There are various types of protocols used over networks, such as http for making and receiving request about a domain name, POP, IMAP, SMTP for email communication, VoIP for Internet telephony, and so on.

In the following lines, we are briefly talking about some protocols that are used on the Internet for various different purposes.

1. HTTP (Hypertext Transfer Protocol)

The **Hypertext Transfer Protocol** (HTTP) is an application-level protocol with the lightness and speed necessary for distributed, collaborative, hypermedia information systems. It is a generic, stateless, object-oriented protocol which can be used for many tasks.

Practical information systems require more functionality than simple retrieval, including search, front-end update, and annotation. HTTP allows an open-ended set of methods to be used to indicate the purpose of a request. It builds on the discipline of reference provided by the *Uniform Resource Identifier* (URI), as a *location* (URL) or *name* (URN), for indicating the resource on which a method is to be applied. Messages are passed to HTTP in a format similar to that used by Internet Mail and *Multipurpose Internet Mail Extensions* (MIME). HTTP is also used as a generic protocol for communication between user agents and proxies/gateways to other Internet protocols, such as SMTP, NNTP, FTP, Gopher and WAIS, allowing basic hypermedia access to resources available from diverse applications and simplifying the implementation of user agents.

The HTTP protocol consists of two fairly distinct items : the set of requests from browsers to servers and the set of responses going back to the other way.

The HTTP has various built-in request methods which allow users to read a web page, or to read a web page's header, or to store a webpage, or to append to a named resource, or to remove the web page or to connect two existing resources or to break an existing connection between two resources.

2. FTP (File Transfer Protocol)

One of the original services on the Internet was designed to allow for transferring files from one system to another. It goes by the name *ftp* which stands for *file transfer protocol*. Files of any type can be transferred, although you may have to specify whether the file is an ASCII or binary file. They can be transferred to any system on the Internet provided that permissions are set accordingly.

FTP offers these advantages :

(*i*) It is very useful to transfer files from one network in an organization to another.

(*ii*) It is an effective way to get a geographically dispersed group to co-operate on a project.

(*iii*) It is a potent and popular way to share information over the internet.

NOTE

FTP (File Transfer Protocol) is a standard for the exchange of files across Internet.

FTP isn't just the name of the protocol ; it is also the name of a program or command. Issue the command by typing *ftp* followed by the address of another site, and press enter.

FTP works as a client/server process. You give the command *ftp* using a remote address such as the following :

FTP newday.horizon com

The above command means that the ftp running on your system is client to an *FTP* process that acts as server on *newday.horizon.com*. You can issue commands to the ftp process at *newday*, and it will respond appropriately.

This protocol is mainly concerned with the transfer of files.

Objectives of FTP are :

- to promote sharing of files (computer programs and/or data) ;
- to encourage indirect or implicit (via programs) use of remote computers ;
- to shield a user from variations in file storage systems among hosts ; and
- to transfer data reliably and efficiently. FTP, though usable directly by a user at a terminal, is designed mainly for use by programs.

3. POP (Post Office Protocol)

POP3, *i.e.*, the **Post Office Protocol** version 3 has become a standard mail protocol. The POP3 defines the rules about receiving emails from a remote server to a local email client. It also makes it possible for the users to download their received email messages onto their local computer so that they can read them even when they are not connected to the Internet (offline reading). POP3 protocol is suitable if you are accessing your emails using a single application or from a single location.

By default, the POP3 protocol works on *two* ports :

Port 110 – the default POP3 non-encrypted port, ***used for unsecured email communication.***

Port 995 – the encrypted port ***used for secure email communication*** using POP3.

NOTE

By default, POP3 deletes emails on the server after downloading them to your local email client.

4. IMAP (Internet Message Access Protocol)

The **Internet Message Access Protocol (IMAP)** is another mail protocol used in conjunction with POP3 protocol for accessing emails on a remote web server and downloads them to a local client. Contrary to POP3 that assumes that single application will access the email, IMAP supports multiple applications, even multiple clients and multiple locations.

NOTE

IMAP is more suitable for you if you're going to access your email from different locations or if your messages are managed by multiple users.

By default, the IMAP protocol works on two ports :

Port 143 – the default, non-encrypted port (unsecure communication).

Port 993 encrypted port used for secure communication.

5. SMTP (Simple Mail Transfer Protocol)

While POP3 and IMAP protocols are used for fetching emails from the email server to client application, the SMTP (Simple Mail Transfer Protocol) is used for sending emails across the Internet.

By default, the SMTP protocol works on these ports :

Port 25 – the default, SMTP non-encrypted port (unsecure).

Port 465 – encrypted port (secure communication).

6. VoIP (Voice over Internet Protocol)

VoIP is a technology that enables voice communications over the Internet through the compression of voice into data packets that can be efficiently transmitted over data networks and then converted back into voice at the other end. Data networks, such as the Internet or local area networks (LANs), have always utilized packet-switched technology to transmit information between two communicating terminals (for example, a PC downloading a page from a web server, or one computer sending an e-mail message to another computer).

The most common protocol used for communicating on these packet-switched networks is Internet protocol, or IP. VoIP allows for the transmission of voice along with other data over these same packet-switched networks and provides an alternative to traditional telephone networks, which use a fixed electrical path to carry voice signals through a series of switches to a destination.

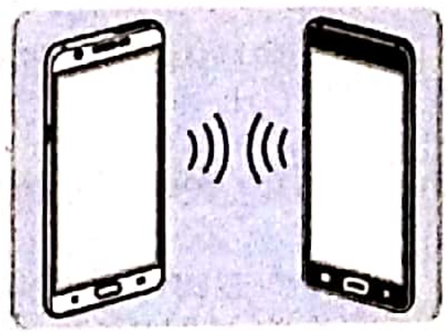
7. NFC (Near Field Communications)

NFC protocol is used to provide short-range wireless connectivity between two electronic devices that within the distance of 4-5 centimetres. It does not require special set-up like other type of wireless communication and establishes a two-way contactless connection between two electronic devices. Once NFC connection is established, the two connected device can share the digital content.

NFC connection is inherently more secure because it is established only when two NFC supporting devices come closer to one another. It is not a stealth connection and hence a secure one. NFC utilises inductive-coupling, at a frequency of 13.56 MHz, which is a licence free allocation in the HF portion of the radio spectrum.

NOTE

As no physical connectors are used with NFC near field communication, the NFC connection is more reliable.



NFC technology in active mode

12.11 HOW HTTP WORKS – A BASIC IDEA

Whenever you enter a URL in the address box of the browser, the web browser displays the intended URL's website or sometimes an error message. Internally, the web browser translates the URL into a request message according to the specified protocol; and sends the request message to the server. The web browser is the HTTP client here.

Protocol HTTP works over the protocol TCP/IP. The HTTP protocol uses a client-server communication model to facilitate the exchange of information on the web. There are HTTP

clients that make requests via HTTP protocol and **HTTP servers** that respond to HTTP requests. In other words, the web communication between a host and a client occurs, via an HTTP request/response pair.

NOTE

The client initiates an HTTP request message, which is serviced through a HTTP response message in return.

Let us now see HTTP actually works.

(*i*) For web communications, the request message (HTTP request), is sent to an HTTP server in the form of URLs (Uniform Resource Locators) by the HTTP client.

(*ii*) The HTTP server receives the HTTP request, fetches the information as per the request and sends it to the HTTP client. This is called the response message from HTTP server.

NOTE

HTTP is a pull protocol, *i.e.*, the client pulls information from the server (instead of server pushes information down to the client).

(*iii*) The HTTP client (the browser) receives the response message, interprets the message and displays the contents of the message on the browser's window (which could be either the website or an error message if such URL does not exist)

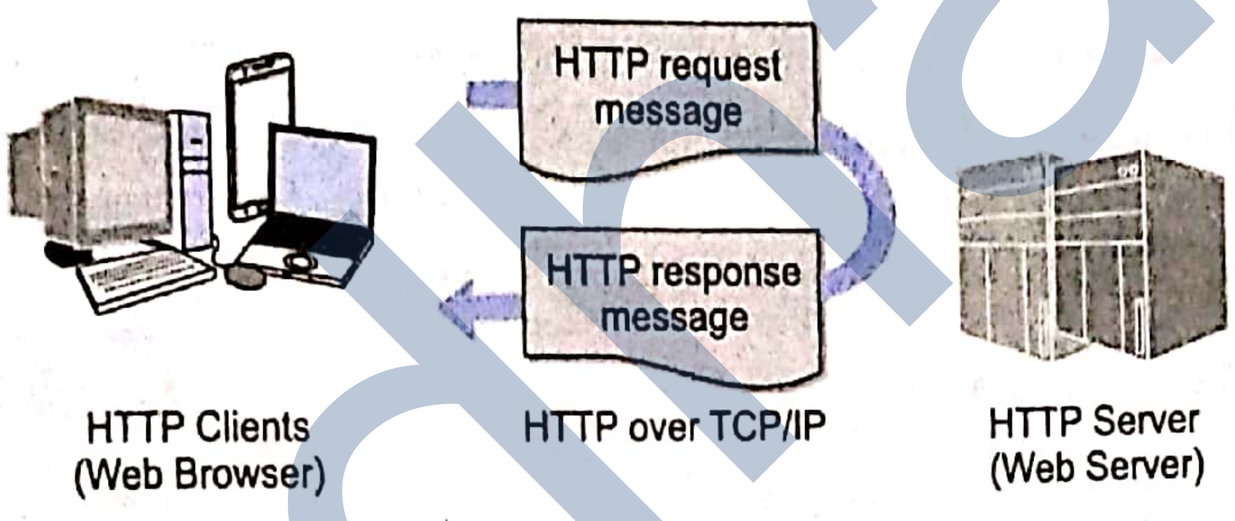


Figure 12.8 Working of HTTP.

HTTP is a stateless protocol. In other words, the current request does not know what has been done in the previous requests.

12.12 WORKING OF EMAIL

You have been writing, sending and receiving emails. What happens after you click the send button of your email, have you ever thought ? No ? Well, read on then.

(*i*) You compose and send an email from your email client. Your email has the recipient's email address along the email message.

(*ii*) Now your email client connects to the **Outgoing SMTP server** and hands over the email message in the required format[3].

(*iii*) The **Outgoing SMTP** first validates the sender details and if valid processes the message for sending and places it in Outgoing queue.

(*iv*) Next DNS look up takes place. The SMTP server based on the domain details in the recipient address, looks up the DNS server of the domain and retrieves the Recipient server information (such as MX records) of the recipient domain.

Mail Exchange (MX) records are DNS records that are necessary for delivering email to the recipient's address.

3. in MIME (Multipurpose Internet Mail Extension) format.

(*v*) Then the SMTP server connects with the Recipient email server and sends the email through SMTP protocol.

(*vi*) The Recipient server in turn validates the recipient account and delivers the email to the users mail account.

(*vii*) The user logs into own email account and views the received email using *email client* that will use POP3/IMAP protocols.

For example, you have sent an email from your email account **abc@gmail.com** to **xyz@edup.com**. Once you click send button :

(*a*) Your email client contacts SMTP server of Gmail (since your email account is on gmail.com)

(*b*) The SMTP server at Gmail checks your email for recipient's email address and the recipient's address **xyz@edup.com** is extracted.

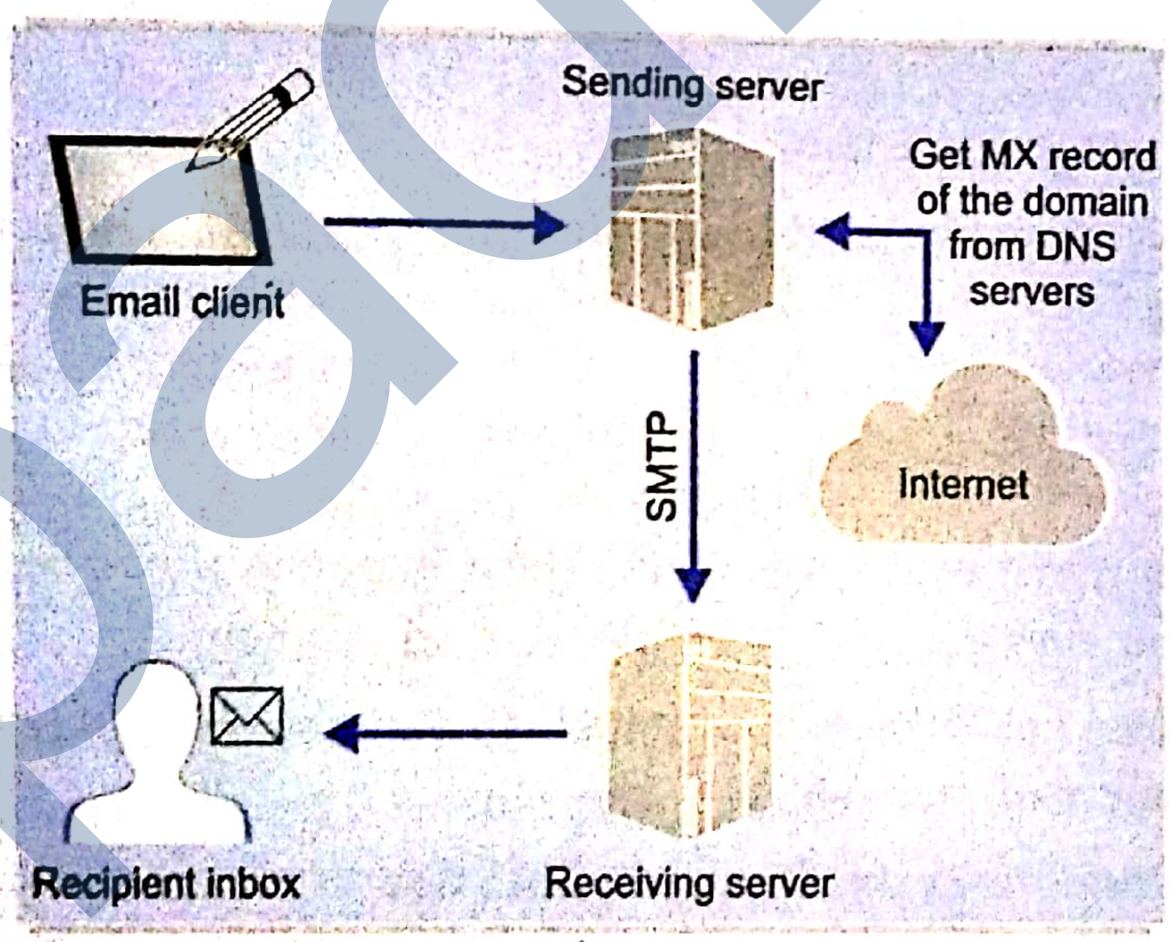
(*c*) Next, the Gmail SMTP server looks for the MX (mail exchange) record of edup.com from DNS.

(*d*) Now the GMAIL's SMTP server will retrieve the address of **SMTP server of edup.com** from its MX record and sends the email to SMTP server of **edup.com**.

(*e*) The SMTP server of edup.com receives the email message.

(*f*) The SMTP server of edup.com checks if the **'xyz'** recipient exists on that server (edup.com). If the account exists on that server, it forwards the email to its own IMAP/POP3 server (mail delivery agent) to store this email.

Figure 12.9 explains this process.



NOTE

Mail Exchange (MX) records are DNS records that are necessary for delivering email to the recipient's address.

Figure 12.9 Working of an email.

12.13 SECURE COMMUNICATION

Sharing information is the paramount feature of the web, and the very feature makes it vulnerable to attacks and makes it insecure too. Every day people share lots of private information such as *banking information (net banking), credit/debit cards details for online payments, login ids and passwords* for various types of accounts such as social media accounts, email accounts, and so forth. This information is so important and private that this must be securely exchanged over the web and it must not fall into the hands of people with malicious intentions.

To ensure the safety of the information being transmitted over the web, many Internet security measures are employed. **Encryption** is one of such measures and is highly recommended too. Encryption is a technique that translates the original data into a form which is not a usable form of data. The encrypted data must be decoded or decrypted to bring it back to the original form. To decrypt the data, a specific code called **the decryption key** is required. Only the people that have access to this secret code (the decryption key) can decode and read the actual data.

ENCRYPTION

Encryption is a technique that translates the original data into a form which is not a usable form of data. The encrypted data must be decoded or decrypted to bring it back to the original form.

Crucial data's safety is ensured by the use of a protocol called HTTPS (HTTP Secure), which transfers the data in encryption form so that eavesdroppers cannot make use of it.

12.13.1 HTTPS

HTTPS stands for **HyperText Transfer Protocol Secure** and is a combination of HTTP and SSL/TLS protocols. HTTPS provides encrypted communication and secure identification of a network web server. HTTPS encrypts your data and establishes a secure channel over a non-secure network to ensure protected data-transfer. Thus data is protected from eavesdroppers and hackers who want to intercept and access your data. That is why most banks apply HTTPS because HTTPS connections are more secure for online payment transactions compared to HTTP connections.

How to check if your connection is secure ?

Before keying in any personal /financial information on any website, make sure that the URL starts with "HTTPS" and that there is a padlock sign [🔒] on the navigation bar or footer of your browser as shown below :

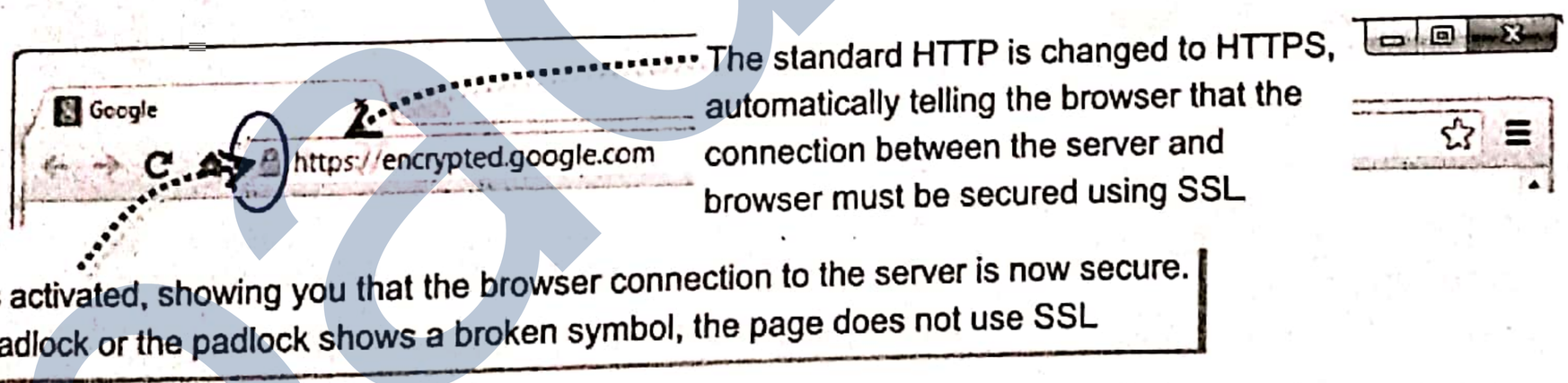


Figure 12.10 Indicators of HTTPS/SSL usage

12.13.2 Secure Sockets Layer (SSL)

SSL stands for **Secure Sockets Layer** protocol. It is a mechanism of data transfer over Internet to provide a safe passage for the transmission of data – like transferring a message inside a locked safe. It encrypts (*i.e.*, converts into un-understandable form) the data so that a third party cannot eavesdrop on the transmission and view the data being transmitted.

How SSL works ?

The working of SSL requires that the website has SSL certificate installed which ensures its authenticity. Once installed, the sensitive information (such as ***Credit card details, Login and password*** details etc.) is obtained from the user through a secure connection over Internet. Without SSL, the attackers can try to steal personal information given to site.

Following Fig. 12.11 illustrates the working of SSL

1. 

Mr. Sachin K.

I run a small business namely **Sachin Sales** to get orders online & Get payments online.

He has a website say SachinSales.com

2. Sachin needs to apply for SSL Certificate from a competent Authority (CA) (such as GlobalSign)

3. The CA people do some kind of investigation to make sure :
   - Sachin K. is a real person
   - Sachin Sales is a real business
   - SachinSales.com is the real site representing business Sachin Sales

4. Once investigated, SSL Certificate is issued to SachinSales.com, which is installed at its web server.

(*a*) Background Work

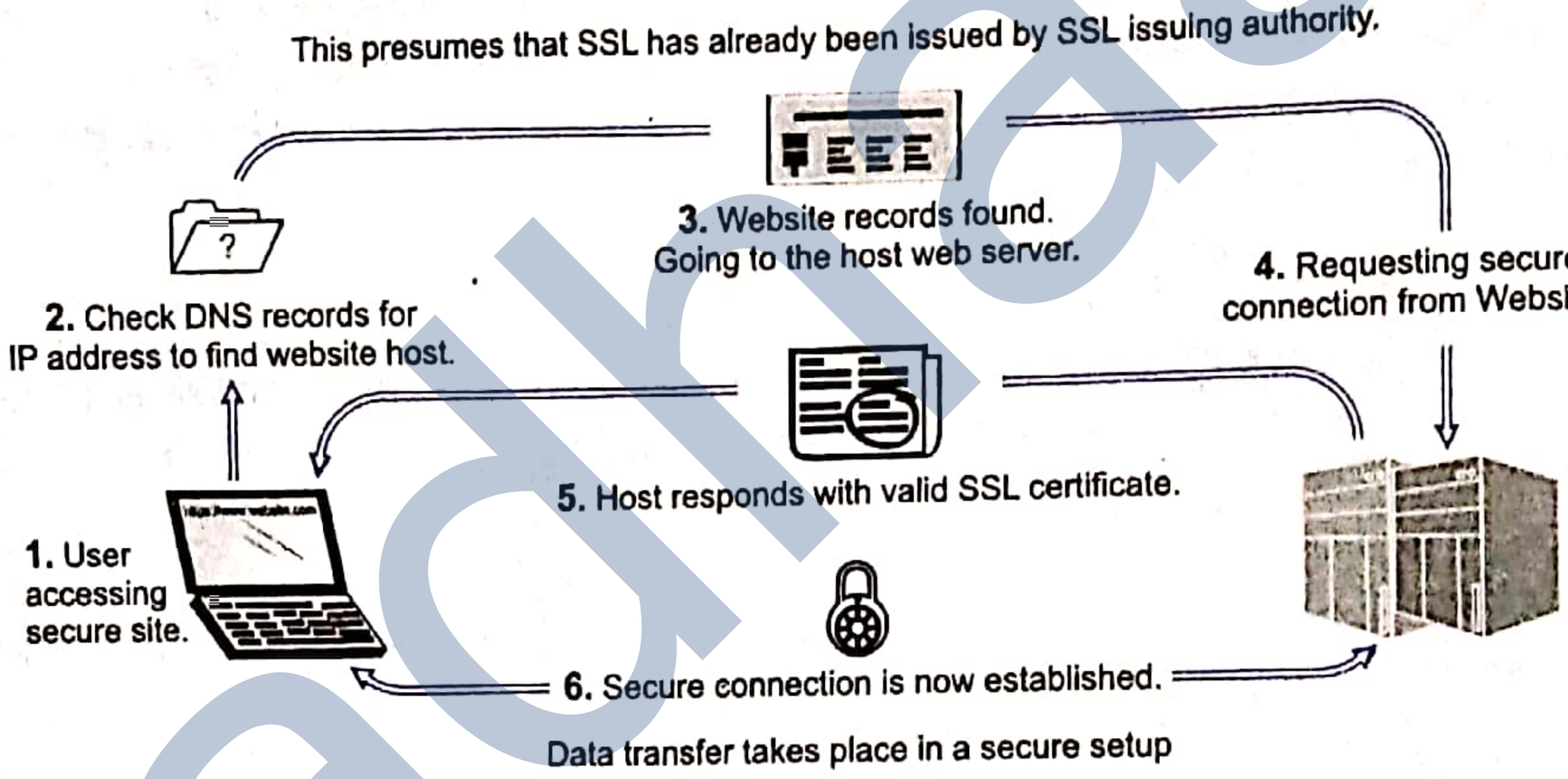


Figure 12.11 Working of SSL (*b*) Secure Transaction over Internet.

Indicators of SSL Usage

SSL shows some marks/ signs when establishing a secure session with the end user. In the case of a browser for instance, users are alerted to the presence of SSL when the browser displays a ***padlock***, or, in the case of Extended Validation SSL, when the address bar displays both a padlock and a green bar. (*see* Fig. 12.12)

SSL protocol works in collaboration with the other protocols, which are HTTP and TCP.

The standard HTTP is changed to HTTPS, automatically telling the browser that the connection between the server and browser must be secured using SSL.

The padlock is activated, showing you that the browser connection to the server is now secure. If there is no padlock or the padlock shows a broken symbol, the page does not use SSL.

Figure 12.12 Indicators signs of SSL.

12.14 NETWORK APPLICATIONS

Computer Networks have connected computers all over the world in a way that it is now possible to work on a computer even if you are not physically present next to it. Two network applications that make such an access possible are : **remote desktop** and **remote login.**

Remote Desktop

The remote desktop is a type of network application through which a person can work on the desktop of another computer (which is at a different location) in the same manner as if that computer is right in front of the person. The person connects to the remote computer (called the **host computer**) via own computer (**the client computer**) on which s/he is working. For instance, you are working on an important project when you fell ill. The doctor has advised you not to travel, but you can work from home. This time, you would want to connect to your work computer (the host computer) while sitting at your home, working on your home laptop (the client computer) using the remote desktop application.

REMOTE DESKTOP CONNECTION

Remote Desktop Connection is a technology that allows you to sit at a computer (the client computer) and connect to a remote computer (the host computer) in a different location.

The remote desktop application displays the desktop of the host computer on the screen of the client computer, and the user can work on it as if it is his/her computer.

Check Point 12.1

1. Define modulation.
2. Name two commonly used modulation techniques.
3. What is modulated wave ?
4. What is collision in a network ?
5. What type of duplex communication take place in wireless networks ?
6. Name some common error checking techniques used in networks.
7. Define checksum.
8. What is routing ?
9. What is a URL and an IP address ?
10. What is DNS.
11. What is a protocol ?
12. How does TCP react when there is congestion in a network ?
13. What are the full forms of these ?
    (*i*) HTTP, (*ii*) HTTPS, (*iii*) FTP,
    (*iv*) SSH (*v*) SSL, (*vi*) POP
    (*vii*) IMAP (*viii*) SMTP (*ix*) VoIP
14. What are MX records ?
15. What is encryption ? Why is it important for transmission over a network ?
16. Describe remote desktop.
17. Describe remote login.

Remote Login

The remote login is a network application that permits a user sitting at a different location to work on a specific program on another computer. The work access to a program is granted by login concept wherein users having authorised login and password to work on that program are allowed access.

There are two programs: TELNET and SSH that facilitate remote login on the Internet. You specify the remote machine on which you want to work, and these programs will help you connect to it. After entering valid login details, you are allowed access to the application program you want to work on. The local application program you are accessing the remote machine is the client. Whatever keystrokes and mouse movements you perform on the client program, it sends them to the remote device, and the remote computer sends the output as per sent keystrokes/ mouse movements. The output received is then displayed the screen of the client.

Remote login is different from accessing the information over the Internet. It is not just the data transfer that is taking place one way; it is an interactive data transfer where the user is interacting with the remote program.

REMOTE LOGIN

A **remote login** facility permits a user to work on a program on a distant computer based on valid login credentials.

LET US REVISE

- ***Modulation** is a process of changing the characteristics of the carrier wave by superimposing the message signal on the high frequency signal.*
- *In **Amplitude Modulation**, the strength of the carrier signal, i.e., the amplitude, is varied as per the changes in the amplitude of the modulating signal.*
- *In **Frequency Modulation**, the frequency of the carrier signal is varied as per the changes in the amplitude of the modulating signal.*
- ***Modulation** is the technique of changing the characteristics of the signal being transmitted so that it carries data and **Demodulation** is the reverse process of modulation where data is extracted from the received signal.*
- *In Full duplex connections, the sending and receiving of signals can take place simultaneously. In half duplex either sending takes ore receiving takes place at a time not simultaneously.*
- *In a computer network, collision is a specific condition that occurs when two or more nodes on a network transmit data at the same time.*
- *CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) is a protocol used by wireless networks to avoid collisions during transmission.*
- *There are two forms of CSMA/CA : (i) CSMA/CA with ACK and (ii) CSMA/CA with RTS/CTS.*
- *CSMA/CA with ACK is employed in small networks and CSMA/CA with RTS/CTS is employed in bigger networks.*
- *To detect/check errors on the Internet, various techniques are used such as single dimensional parity check, two dimensional parity check and checksum etc.*
- *The checksum refers to a sum of data bits calculated from digital data that is used to ensure the data integrity at the receiver's end.*
- *Routing is the process of efficiently selecting a path in a network along which the data packets will travel to their destination.*
- *A router maintains a table called the routing table which stores the routing information which is about the best routes to other networks from that router.*
- *Network congestion is a specific condition in a network when more data packets are coming to network devices than they can handle and process at a time.*
- *Metering or rate modulation technique is implemented to control the network congestion in which the incoming traffic to a router is controlled.*
- *Common cellular/wireless network connectivity protocols are 2g, 3g, 4g, WiFi.*
- *Basic network tools that help you determine the status of a network are ping, traceroute, nslookup, ipconfig, whois etc.*
- *Common network protocols are HTTP, FTP, POP/IMAP, SMTP, VoIP, NFC etc.*
- *HTTP works over the TCP protocol where the client initiates an HTTP request message, which is serviced through a HTTP response message in return.*
- *Encryption is a technique that translates the original data into a form which is not a usable form of data. The encrypted data must be decoded or decrypted to bring it back to the original form.*
- *HTTP with encryption along with SSL is used by HTTP protocol.*
- *To work on distant computers over the Internet, there are two common network applications: remote desktop and remote login.*

Solved Problems

1. *What is modulation ?*

   Solution. The process of altering the characteristics (amplitude or frequency etc.) of a high-frequency wave called the carrier wave so that it can carry low-frequency information along with it while being transmitted, is called **modulation**.

2. *What is carrier wave ? What is modulated wave ?*

Solution. The high frequency wave whose characteristics are altered to superimpose message information, is the **carrier wave** and after altering the characteristics, the new resultant wave is called the **modulated wave.**

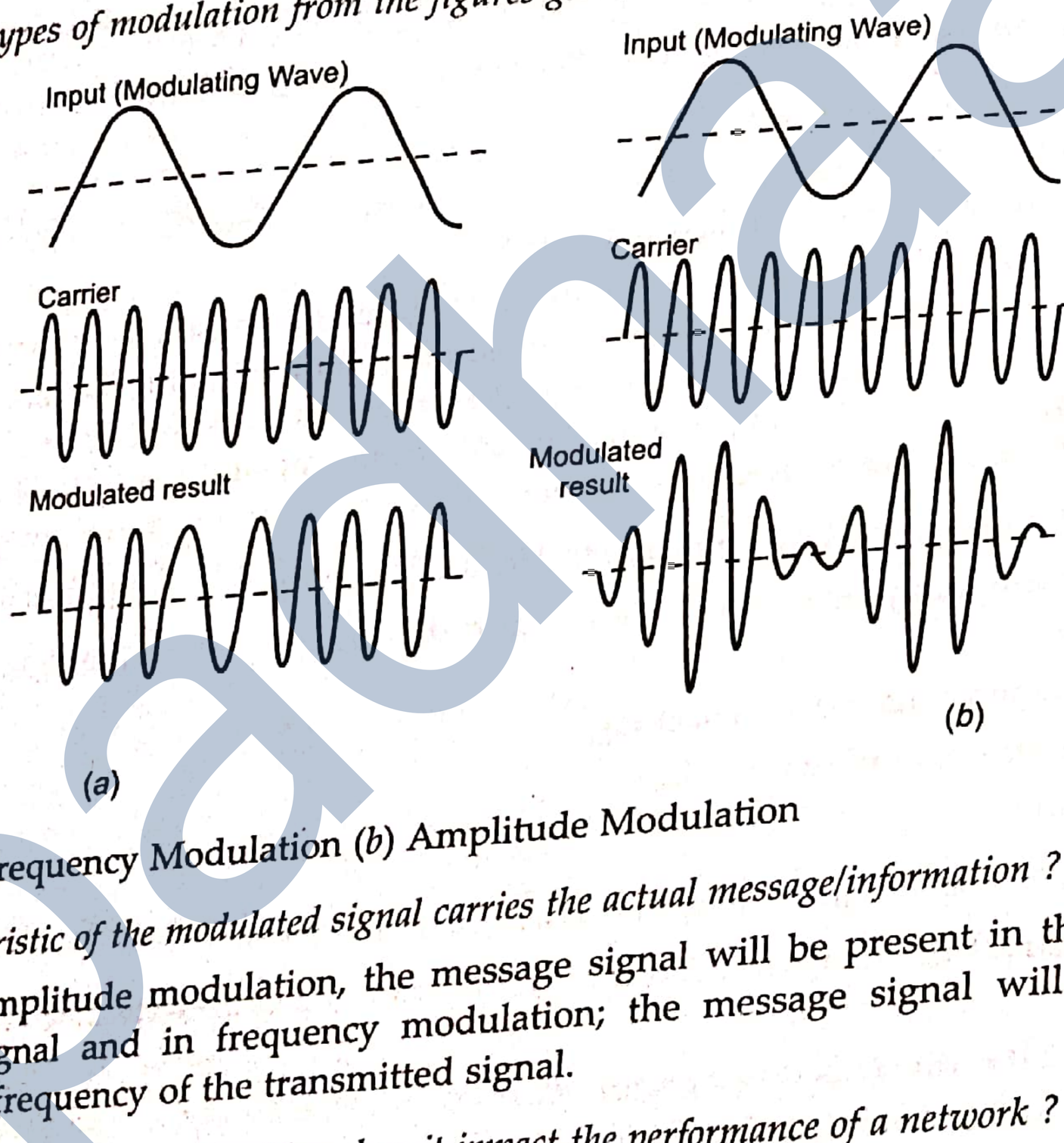
3. *What is amplitude modulation ?*

Solution. When a high-frequency carrier wave's amplitude is varied in accordance with the information to be transmitted, keeping the frequency and phase of the carrier wave unchanged, this process is called Amplitude Modulation.

4. *What is demodulation ? How is it different from modulation ?*

Solution. Modulation is the technique of changing the characteristics of the signal being transmitted so that it carries data and Demodulation is the reverse process of modulation where data is extracted from the received signal (*i.e.*, from the modulated wave).

5. *Identify the types of modulation from the figures given below :*



Solution. (*a*) Frequency Modulation (*b*) Amplitude Modulation

6. *Which characteristic of the modulated signal carries the actual message/information ?*

Solution. In amplitude modulation, the message signal will be present in the amplitude of the transmitted signal and in frequency modulation; the message signal will be present in the instantaneous frequency of the transmitted signal.

7. *What is a collision in a network ? How does it impact the performance of a network ?*

Solution. In a computer network, collision is a specific condition that occurs when two or more nodes on a network transmit data at the same time. In case of a collision, the data gets garbled and cannot be read. Also, it may hamper the overall performance of the network as collisions often lead to more retransmissions which clog the network and deteriorate the overall performance of the network.

8. *What measures do wireless networks employ to avoid collisions ?*

Solution. The wireless networks employ a protocol called CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) to avoid collisions in the network.

9. *Explain the two types of duplex communication.*

Solution. There are mainly two types of duplex communication :

(*i*) **Full duplex.** In this type of transmission, two bit streams can be simultaneously transmitted over the links at the same time, one going in each direction, *i.e.*, sending as well as receiving the data.

(*ii*) **Half duplex.** In this type of transmission, data can flow in only one direction at a time *i.e.*, either sending or receiving of data at a time.

10. *The wireless networks employ strategies to avoid collisions. Why can't they detect collisions ?*

Solution. Collisions occur when multiple transmissions take place at the same over a network. Wireless networks are half duplex in nature, *i.e.*, they cannot listen while transmitting (and while listening, they cannot transmit – only one operation at a time). Hence they cannot find out if any other transmission is taking place simultaneously, and thus cannot detect collisions.

11. *What is CSMA/CA ?*

Solution. Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA) is a media access protocol that is related to CSMA/CD and is also used on multiple access networks.

12. *What is CSMA/CA ? How does it work ?*

Solution. Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA) is a media access protocol that is used on multiple access wireless networks.

With CSMA/CA, a device listens for an opportunity to transmit its data, *i.e.*, CARRIER SENSE. If the carrier is free, the sending device does not immediately transmit data. Rather, it first transmits a signal notifying other devices (*i.e.*, a warning packet) that it is transmitting for so much time before actually sending the data. The other device refrains from transmitting data for the specified time limit. This means data packets will never collide, although warning packets might.

13. *What are basic methods of checking errors in the data being transmitted over networks ?*

Solution. There are many methods of checking or detecting errors in the data transmitted. Three simplest ones are :

(*i*) Single dimensional parity checking

(*ii*) Two dimensional parity checking

(*iii*) Checksums

14. *What types of errors may occur in the data transmitted over networks ?*

Solution. The errors that may occur in the data transmitted over networks, can be one or more of following types:

(*i*) **Single-bit error.** This type of error occurs if only one bit of the transmitted data got changed from 1 to 0 or from 0 to 1.

(*ii*) **Multiple-bit error.** This type of error occurs if two or more nonconsecutive bits in data got changed from 0 to 1 or from 1 to 0.

(*iii*) **Burst Error.** This type of error occurs if two or more consecutive bits in data got changed from 0 to 1 or from 1 to 0.

15. *What do you understand by parity checking ?*

Solution. Parity checking is a method of error detection that can check 1 or 2 bit errors (but not all of these). In parity checks, a parity bit is added to the end of a string of binary code to indicate whether the number of bits in the string with the value 1 is **even** or **odd**.

There can be *two* types of parity bits :

- **Even parity bit** where the parity bit is set to 1 if the number of bits is odd. The extra parity bit will make the number of 1s even.
- **Odd parity bit** where the parity bit is set to 1 if the number of bits is even. The extra parity bit will make the number of 1s odd.

For example, if we have data as 0101010 , then

- With even parity it becomes 01010101 (because 0101010 has 3 bits that are 1, so using even parity the parity bit is 1 to make the number of 1's as an even number)
- With odd parity it becomes 01010100 (since the number of 1's are already 3, no need to add another 1 to make it odd, hence the parity bit is 0)

Data is transmitted along with the parity bit. The receiver recalculates the parity from the data part only extracting the parity bit and then compares the calculated parity bit with the received parity bit. If they match, the data is considered to be correct and accepted.

16. *Give an example of how 1 two-dimensional parity check detects error in the received data ?*

Solution. Two-dimensional parity can detect all 1 and 2 bit errors, and recover from all 1 bit errors. The data bits are arranged in a grid, and parity is computed for each row and column.

For example,

```
1  0  0  1  |  0
1  1  0  0  |  0
0  1  1  0  |  0
0  1  1  1  |  1
---------+----
0  1  0  0  |  0
```

A single bit error will cause a parity violation in exactly one row and one column. The intersection of that row and column must contain the incorrect bit :

```
1  0  0  1  |  0
1  1  0  0  |  0
0  1 [0] 0  |  0   <-- does not match
0  1  1  1  |  1
---------+----
0  1  0  0  |  0
      ^
      |
does not match
```

A two bit error will cause parity violations in either :

- two rows and two columns
- two rows (if the errors occur in the same column)
- two columns (if the errors occur in the same row)

17. *What are the steps followed in checksum generator ?*

Solution. The sender, which is the checksum generator, follows these steps :

(*a*) The units are divided into *k* sections each of *n* bits.

(*b*) All sections are added together using 1's complement to get the sum.

(*c*) The sum is complemented and become the checksum.

(*d*) The checksum is sent with the data.

18. *Consider the following data being transmitted where each data unit contains two bytes of data :*

```
11001111    10011100
10100100    00111011
01100100    01101010
10100011    00010010
11010001    01001101
```

Considering even parity, determine how the data will be transmitted along with two-dimensional parities.

Solution. Considering two-dimensional even parity, the data will be sent as shown below :

```
11001111    10011100    0
10100100    00111011    0
01100100    01101010    1
10100011    00010010    0
11010001    01001101    0
01111101    10010010    1
```

19. *With a two-dimensional even parity check employed, following data is received. The data contains some errors. Can you pinpoint the erroneous bit?*

```
11001111    10011100    0
10100100    00111011    0
01100100    01100010    1
10100011    00010010    0
11010001    01001101    0
01111101    10010010    1
```

Solution. Upon recalculating the parity bits from the received data

```
11001111    10011100    0    0
10100100    00111011    0    0
01100100    01100010    0    1
10100011    00010010    0    0
11010001    01001101    0    0
01111101    10011010         0
01111101    10010010         1
```

The intersecting bit is erroneous bit

ERROR

20. *What are checksums ?*

Solution. Checksum is an error detection technique used for checking errors in the received data.

In this technique, at the transmitter's end, as the device transmits data, it takes the sum of all of the data elements it is transmitting to create an aggregate sum. This sum is called the **datasum**. The overflow carries generated by the additions are added back into the *datasum*. The transmitting device then sends a form of this **datasum** appended to the end of the block. This new form of the *datasum* is called the **checksum.**

At the receiver end, as the data elements are received, they are added a second time in order to recreate the *datasum*. Once all of the data elements have been received, the receiving device compares its calculated *datasum* with the checksum sent by the transmitting device.

If both these match, the data is considered error-free and accepted otherwise rejected.

21. *What is ACK(Acknowledgement) signal ?*

Solution. The acknowledgement signal or the ACK signal is a control code, which is sent by the receiving computer to indicate that the data has been received without error and that the next part of the transmission may be sent.

22. *Consider following data units that are to be transmitted along with checksum information.*

```
1000  0110  0101  1110
1010  1100  0110  0000
0111  0001  0010  1010
1000  0001  1011  0101
```

In what form will the data be transmitted ?

Solution. In order to calculate the checksum, the data units are to be added using 1's complement where the overflow bit is to be added back to the sum.

One by one all data units are to be added *i.e.,* :

```
     1000 0110 0101 1110      First 16-bit value
+    1010 1100 0110 0000      Second 16-bit value
----------------------
 1   0011 0010 1011 1110      Produced a carry-out, which gets added back
+                        1
----------------------
     0011 0010 1011 1111      Third 16-bit value
+    0111 0001 0010 1010
----------------------
 0   1010 0011 1110 1001      No carry to swing around (**)
+    1000 0001 1011 0101      Fourth 16-bit value
----------------------
 1   0010 0101 1001 1110      Produced a carry-out, which gets added back
+                        1
----------------------
     0010 0101 1001 1111      Our final datasum"
```

Taking complement of the datasum will give us the checksum.

```
0010 0101 1001 1111      's complement will be:
1101 1010 0110 0000      This is our checksum
```

Now the data will be transmitted in the following form :

```
1000 0110 0101 1110
1010 1100 0110 0000
0111 0001 0010 1010
1000 0001 1011 0101
1101 1010 0110 0000
```

23. *What is routing ? Explain briefly.*

Solution. Routing is the process of selecting paths to move information across networks from the source network to the destination network.

When a data packet reaches a router, the router selects the best route to the destination network from its routing table and forwards the data packet to the neighbouring router as per the selected best route. This way each router keeps passing the data packet(s) to its neighbouring router on best route to the destination and finally the data packet reaches its destination.

24. *What is routing table ? What type of information is stored in a routing table ?*

Solution. Routing table is a table maintained by each router where it records the next hop for the best route to a destination. Routing information such as the *destination network, metric* (such as cost), and *next hop* etc., are stored on a routing table.

25. *What is network congestion ? What are the symptoms of network congestion ?*

Solution. Network congestion is a specific condition in a network when more data packets are coming to network devices than they can handle and process at a time.

Networks identify the congestion situation through the following symptoms :

(*i*) excessive packet delay (*ii*) loss of data packets (*iii*) retransmission.

26. *What are protocols ? What is the significance of protocols in networks ?*

Solution. A **protocol** is a system of rules that allow two or more entities of a communications system to transmit information via any kind of variation of a physical quantity. For example, there are protocols for the data interchange at the hardware device level and protocols for data interchange at the application program level.

Network protocols govern the end-to-end processes of timely, secure network communication. Network protocols incorporate all the processes, requirements and constraints of initiating and accomplishing communication between computers, servers, routers and other network enabled devices.

27. *Write a brief note on TCP/IP suite.*

Solution. Transmission Control Protocol/Internet Protocol, TCP/IP is a set of rules (protocols) governing communications among all computers on the Internet. More specifically, TCP/IP dictates how information should be packaged (turned into bundles of information called packets), sent, and received, as well as how to get to its destination.

The TCP/IP Internet protocols consist of :

- **Transmission Control Protocol (TCP)**, which uses a set of rules to exchange messages with other Internet points at the information packet level.
- **Internet Protocol (IP)**, which uses a set of rules to send and receive messages at the Internet address level.

TCP/IP is able to integrate and interacts with additional Internet protocols that include the UDP(User Datagram Protocol), Hypertext Transfer Protocol (HTTP) and File Transfer Protocol (FTP), each with defined sets of rules to use with corresponding programs elsewhere on the Internet.

28. *Write a short note on IPv4 addressing.*

Solution. An IPv4 address consists of a series of 32 binary bits (ones and zeros). The 32 bits are grouped into four segments of 8 bits called **octets**. Each octet is presented as its decimal value, separated by a decimal point or period. This format is referred to as **dotted-decimal notation**. When a host is configured with an IPv4 address, it is entered as a dotted-decimal number, such as 192.168.1.5.

29. *Discuss how IPv4 is different from IPv6.*

Ans. Internet Protocol (IP) is a set of technical rules that define how computers communicate over a network. There are currently *two* versions : **IP version 4** (IPv4) and **IP version 6** (IPv6).

- IPv4 was the first version of Internet Protocol to be widely used and still accounts for most of today's Internet traffic. There are just over 4 billion IPv4 addresses. While that is a lot of IP addresses, it is not enough to last forever.
- IPv6 is a newer numbering system to replace IPv4. It was deployed in 1999 and provides far more IP addresses, which should meet the need well into the future.

The major difference between IPv4 and IPv6 is the number of IP addresses. Although there are slightly more than 4 billion IPv4 addresses, there are more than 16 billion-billion IPv6 addresses.

	Internet Protocol version 4 (IPv4)	Internet Protocol version 6 (IPv6)
Address size	32-bit number	128-bit number
Address format	Dotted decimal notation : 192.168.0.202	Hexadecimal notation: 3FFE:0400:2807:8AC9::/64
Number of addresses	2^32	2^128

30. *Which two statements are correct about IPv4 and IPv6 addresses ? (choose two.)*

(*a*) IPv4 addresses are represented by hexadecimal numbers.

(*b*) IPv4 addresses are 32 bits in length.

(*c*) IPv4 addresses are 128 bits in length.

(*d*) IPv6 addresses are represented by decimal numbers.

(*e*) IPv6 addresses are represented by hexadecimal numbers.

(*f*) IPv6 addresses are 32 bits in length.

Solution. (*b*) and (*e*).

31. *Write a short note on IPv6 addressing.*

Solution. An IPv6 address consists of 8 sets of 16-bit hexadecimal values separated by colons (:), totaling 128 bits in length.

For example : `2001:0db8:1234:5678:9abc:def0:1234:5678`

Leading zeros can be omitted, and consecutive zeros in contiguous blocks can be represented by a double colon (::). Double colons can appear only once in the address.

For example : `2001:0db8:0000:130F:0000:0000:087C:140B`

can be abbreviated as

`2001:0db8:0:130F::87C:140B`

32. *Why are protocols needed ?*

Solution. In networks, communication occurs between the entities in different systems. Two entities cannot just send bit streams to each other and expect to be understood. For communication, the entities must agree on a protocol. A protocol is a set of rules that govern data communication.

33. *What is Ping network tool ?*

Solution. The network tool ping sends signals (packets) to another computer on the Internet to see if they send a return or an 'echo.' If all the signals time out, *i.e.*, no response is received, the computer may be disconnected from the Internet or at least unreachable from the server.

This feature only checks if a computer is connected to the Internet, it cannot verify the validity of an e-mail address. It also cannot check a specific web page, but you can check the main server to see if it is connected, *e.g.*, the command

`ping www.edupillar.com/aboutus/`

is not valid, but the command

`ping www.edupillar.com`

is valid.

34. *What is a tracert or traceroute command ?*

Solution. This networking command **traceroute** traces the route through the Internet from the sending device to the destination computer. The signal generally goes from a computer to the Internet Service Provider (ISP) and then to their provider until it reaches a 'backbone' provider. It then eventually transfers to the destination 'backbone' provider and finally reaches to the destination computer.

35. *What is the use of Whois networking command ?*

Solution. The **whois** networking command is used to find the registration records for a specific domain name such as who is the owner of this domain name, when was it registered and till when it is valid, etc.

GLOSSARY

DNS	A way to translate a URL (domain name) into IP address.
Domain Name System	DNS
TCP	Connected oriented protocol that facilitates data transmission over the Internet. A part of TCP/IP protocol stack.
Transmission Control Protcol	TCP
Encryption	Process of converting electronic data to an unrecognizable form.
Protocol	A standard or set of rules that computers and other devices use when communicating with one another.
Bandwidth	The transmission capacity of a communication channel.
Carrier Wave	A signal of chosen frequency generated to carry data ; often used for long distance transmissions.
Decryption	The process of converting encrypted data back into original form.
Full Duplex	Abbreviated FDX. The capability for simultaneous transmission in two directions, so that devices can be sending and receiving data at the same time.
Half Duplex	Abbreviated HDX. The ability to transmit data on the same channel.
Modulation	Process of adding message information on a carrier wave, so that it can be transmitted over long distances.
Routing	The process of directing packets from a network source node to the destination node.
Routing Table	A table stored in a router ; used to keep track of routes to specific network destination.

Assignment

Type A : Short Answer Questions/Conceptual Questions

1. What is modulation ? What is the need of modulation ?
2. What are two main types of modulation techniques ?
3. How is amplitude modulation different from frequency modulation ?
4. What you understand by collisions in a network ?
5. Wired and wireless networks use different mechanisms to detect and handle collisions. Name these.
6. What is CSMA/CA ?
7. Why can't wireless network detect collisions ?

8. What are ACK, RTS, CTS signals ?
9. Explain the working of CSMA/CA and its two implementation.
10. Which implementation of CSMA/CA is used for smaller networks and which one for bigger networks ?
11. What is the process of routing ?
12. What is the importance of routing table in routing ?
13. What is IP addressing ? What are two versions of IP addressing ?
14. How are IPv4 addresses different from IPv6 addresses ?
15. What is Domain name system ? What is DNS look up ?
16. What is URL ? What are the components of a URL ?
17. How is a domain name different from a URL.
18. What is the role and importance of protocols in Networks ?
19. What is the importance of TCP/IP on Internet communications ?
20. What is the role of TCP protocol ? What is the role of IP protocol ?
21. What does TCP do when there is congestion on a network ?
22. What is metering or rate modulation technique used by TCP to avoid congestion in a network ?
23. Discuss following network tools briefly :
    (*i*) traceroute (*ii*) ping (*iii*) ipconfig (*iv*) nslookup (*v*) whois
24. What are protocols ? Why are they important in network ?
25. Discuss following network protocols, briefly :
    (*i*) HTTP (*ii*) FTP (*iii*) SCP (*iv*) SSH (*v*) POP (*vi*) IMAP
    (*vii*) SMTP (*viii*) VoIP (*ix*) NFC
26. Discuss the basic working model of HTTP.
27. What happens behind the scenes when you send an email, before it reaches its destination ?
28. What are MX records ?
29. What is HTTPS ? How does it work ?
30. What is encryption ? Why is considered so important ?
31. What is SSL ? How does it impact the communication over Internet ?
32. What is remote desktop ?
33. What is remote login ?

Type B : Application Based Question

1. Find the erroneous bit(s) in the data transmitted as shown below. Use two-dimensional even parity check.

```
11110000
10101010
11111111
10100101
```

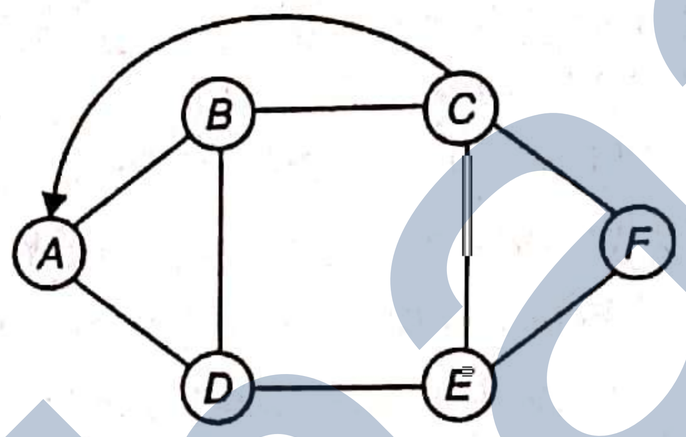
2. Find the erroneous bits in the data transmitted as shown below. Use two-dimensional even parity check.

```
11110000
10111010
11011111
10100101
```

3. Data received by a device is as given below. The data has been sent with a checksum. Find out if the received data is correct or not ?

```
1000 0110 0101 1110
1010 1100 0110 0000
 0111 0001 0010 1001
1000 0001 1001 0101
1101 1010 0110 0000
```

4. Consider the following network map showing how routers of various networks are connected.



Prepare routing tables for any three routers of your choice.