**1. What is a Computer Network?**

Ans: A computer network is a connection network between two or more nodes using Physical Media Links viz., cable or wireless in order to exchange data over pre-configured services and Protocols. A computer network is a collective result of – Electrical Engineering, Computer Science, Telecommunication, Computer Engineering and Information Technology involving their theoretical as well as practical aspects into action. The most widely used Computer Network of Today is Internet which supports World Wide Web (WWW).

**2. What is DNS?**

Ans: DNS stands for Domain Name System. It is a Naming System for all the resources over Internet which includes Physical nodes and Applications. DNS is a way to locate to a resource easily over a network and serves to be an essential component necessary for the working of Internet.

**3. Give a brief description of PAN, LAN, HAN, SAN, CAN, MAN, WAN, GAN.**

Ans: PAN stands for Personal Area Network. It is a connection of Computer and Devices that are close to a person VIZ., Computer, Telephones, Fax, Printers, etc. Range Limit – 10 meters.

LAN stands for Local Area Network. LAN is the connection of Computers and Devices over a small Geographical Location – Office, School, Hospital, etc. A LAN can be connected to WAN using a gateway (Router).

HAN stands for House Area Network. HAN is LAN of Home which connects to homely devices ranging from a few personal computers, phone, fax and printers.

SAN stands for Storage Area Network. SAN is the connection of various storage devices which seems local to a computer.

CAN stands for Campus Area Network, CAN is the connection of devices, printers, phones and accessories within a campus which Links to other departments of the organization within the same campus.

MAN stands for Metropolitan Area Network. MAN is the connection of loads of devices which spans to Large cities over a wide Geographical Area.

WAN stands for Wide Area Network. WAN connects devices, phones, printers, scanners, etc over a very wide geographical location which may range to connect cities, countries and ever continents.

GAN stands for Global Area Network. GAN connects mobiles across the globe using satellites.

**4. What is a router?**

Ans: A router is a physical device which acts as a gateway and connects to two network. It forwards the packets of data/information from one network to another. It acts as an interconnection Link between two network.

**5. What are the use of cross and standard cables? Where do you find their usages?**

Ans: A Network cable may be crossover as well as straight. Both of these cables have different wires arrangement in them, which serves to fulfill different purpose.

Area of application of Straight cable

Computer to Switch

Computer to Hub

Computer to Modem

Router to Switch

Ares of application of Crossover cable

Computer to Computer

Switch to Switch

Hub to Hub

**6. What do you mean by Bandwidth?**

Ans: Every Signal has a limit of its upper range and lower range of frequency of signal it can carry. This range of limit of network between its upper frequency and lower frequency is termed as Bandwidth.

**7.Differentiate between 'attenuation', 'distortion', and 'noise'.**

**Ans.** When a signal travels through a medium, it loses some of its energy due to the resistance of the medium. This loss of energy is called attenuation.

When a signal travels through a medium from one point to another, it may change the form or shape of the signal. This is known as distortion.

Noise is unwanted electrical or electromagnetic energy that degrades the quality of signals and data.

**8. Differentiate between a 'bit rate' and 'baud rate'.**

**Ans.** A bit rate is the number of bits transmitted during one second, whereas, baud rate refers to the number of signal units per second that are required to represent those bits.

Baud rate = bit rate / N, where N is the no. of bits represented by each signal shift.

**9. What is a client/server network?**

**Ans.** In a client/server network, one or more computers act as servers. Servers offer a centralized repository of resources such as printers and files. The client refers to a workstation that has access to the server.

**10. What is the difference between Communication and Transmission?**

**Ans.** Transmission – A process of sending and receiving data between source and destination, in only one way. It is regarded as the physical movement of data.

Communication – A process of sending and receiving data between source and destination, in both ways.

**11. How many layers does TCP/IP have?**

**Ans.** TCP/IP has four layers –

Network Layer

Internet Layer

Transport Layer

Application Layer

**12. differentiate between Firewall and Antivirus?**

**Ans.** Both are security applications used in networking.

A firewall prevents unauthorized access in private networks as intranets. However, it does not protect against virus, spyware, or adware.

An antivirus is a software that protects a computer from any malicious software, virus, spyware, or adware.

**13.What are Unicasting, Anycasting, Multicasting and Broadcasting?**
If the message is sent from a source to a single destination node, it is called Unicasting. This is typically done in networks.

If the message is sent from a source to any of the given destination nodes. This is used a lot in Content delivery Systems where we want to get content from any server.

If the message is sent to some subset of other nodes, it is called Multicasting. Used in the situation when there are multiple receivers of the same data. Like video conferencing, updating something on CDN servers which have a replica of same data.
If the message is sent to all the nodes in a network it is called Broadcasting. This is typically used in Local networks, for examples DHCP and ARP use broadcasting.

**14.What are layers in OSI model?**
There are a total of 7 layers
1. Physical Layer
2. Data Link Layer
3. Network Layer
4. Transport Layer
5. Session Layer
6. Presentation Layer
7. Application Layer

**15.What is Stop-and-Wait Protocol?**
In Stop and wait protocol, a sender after sending a frame waits for an acknowledgment of the frame and sends the next frame only when acknowledgment of the frame has received.

16. **Differences between Hub, Switch and Router?**

| Hub | Switch | Router |
|---|---|---|
| Physical Layer Device | Data Link Layer Device | Network Layer Device |
| Simply repeats signal to all ports | Doesn't simply repeat, but filters content by MAC or LAN address | Routes data based on IP address |
| Connects devices within a single LAN | Can connect multiple sub-LANs within a single LAN | Connect multiple LANS and WANS together. |
| Collision domain of all hosts connected through Hub remains one. i.e., if signal sent by any two devices can collide. | Switch divides collision domain, but broadcast domain of connected devices remains same. | It divides both collision and broadcast domains, |

**17.What is private IP?**

Three ranges of IP addresses have been reserved for private address and they are not valid for use on the Internet. If you want to access internet with these address you must have to use proxy server or NAT server (on normal cases the role of proxy server is played by your ISP.).If you do decide to implement a private IP address range, you can use IP addresses from any of the following classes:

Class A: 10.0.0.0 10.255.255.255
Class B: 172.16.0.0 172.31.255.255
Class C: 192.168.0.0 192.168.255.255

**18.What is public IP address?**

A public IP address is an address leased from an ISP that allows or enables direct Internet communication.

**19.What is the benefit of sub netting?**

It Reduce the size of the routing tables. <

Reduce network traffic. Broadcast traffic can be isolated within a single logical network.

Provide a way to secure network traffic by isolating it from the rest of the network.

20. What is difference between ARP and RARP?

The address resolution protocol (ARP) is used to associate the 32 bit IP address with the 48 bit physical address, used by a host or a router to find the physical address of another host on its network by sending a ARP query packet that includes the IP address of the receiver.
The reverse address resolution protocol (RARP) allows a host to discover its Internet address when it knows only its physical address.

**21.Describe VPN?**

VPN - Virtual Private Network. It is a technology that allows a secure tunnel to be created across a network such as the Internet.

**22.What is DHCP, how does it work?**

The idea of DHCP (Dynamic Host Configuration Protocol) is to enable devices to get IP address without any manual configuration.

The device sends a broadcast message saying “I am new here”

The DHCP server sees the message and responds back to the device and typically allocates an IP address. All other devices on network ignore the message of the new device as they are not DHCP server.

**23. What is the Difference between CSMA/CA and CSMA/CD?**

CSMA/CD:
CSMA/CD stands for Carrier Sense Multiple Access / Collision Detection is a network protocol for carrier transmission. It is operated in the medium access control layer. It senses of the shared channel is busy for broadcasting and interrupts the broadcast until the channel is free. In CSMA/CD collision is detected by broadcast sensing from the other stations. Upon collision detection in CSMA/CD, the transmission is stopped and a jam signal is sent by the stations and then the station waits for a random time context before retransmission.

CSMA/CA:
CSMA/CA stands for Carrier Sense Multiple Access / Collision Avoidance is a network protocol for carrier transmission. Like CSMA/CD it is also operated in the medium access control layer. Unlike CSMA/CD(that is effective after a collision) CSMA / CA is effective before a collision.

Let’s see the difference between CSMA/CA and CSMA/CD:-

| S.NO | CSMA/CD | CSMA/CA |
|---|---|---|
| 1. | CSMA / CD is effective after a collision. | Whereas CSMA / CA is effective before a collision. |
| 2. | CSMA / CD is used in wired networks. | Whereas CSMA / CA is commonly used in wireless networks. |
| 3. | It only reduces the recovery time. | Whereas CSMA/ CA minimizes the possibility of collision. |
| 4. | CSMA / CD resends the data frame whenever a conflict occurs. | Whereas CSMA / CA will first transmit the intent to send for data transmission. |

| S.NO | CSMA/CD | CSMA/CA |
|---|---|---|
| 5. | CSMA / CD is used in 802.3 standard. | While CSMA / CA is used in 802.11 standard. |
| 6. | It is more efficient than simple CSMA(Carrier Sense Multiple Access). | While it is similar to simple CSMA(Carrier Sense Multiple Access). |

**24.Difference between Stop and Wait, GoBackN and Selective Repeat**

Last Updated: 03-12-2018

Reliable data transfers is one of the primary concerns in computer networking. This service department lies in the hands of TCP. There major flow control protocols – Stop and Wait, Go Back N, and Selective Repeat.

**Stop and Wait** –
The sender sends the packet and waits for the ACK (acknowledgement) of the packet. Once the ACK reaches the sender, it transmits the next packet in row. If the ACK is not received, it re-transmits the previous packet again.

**Go Back N** –
The sender sends N packets which is equal to the window size. Once the entire window is sent, the sender then waits for a cumulative ACK to send more packets. On the receiver end, it receives only in-order packets and discards out-of-order packets. As in case of packet loss, the entire window would be re-transmitted.

**Selective Repeat** –
The sender sends packet of window size N and the receiver acknowledges all packet whether they were received in order or not. In this case, the receiver maintains a buffer to contain out-of-order packets and sorts them.The sender selectively re-transmits the lost packet and moves the window forward.

Differences:

| PROPERTIES | STOP AND WAIT | GO BACK N | SELECTIVE REPEAT |
|---|---|---|---|
| Sender window size | 1 | N | N |
| Receiver Window size | 1 | 1 | N |
| Minimum Sequence number | 2 | N+1 | 2N |
| Efficiency | 1/(1+2*a) | N/(1+2*a) | N/(1+2*a) |
| Type of Acknowledgement | Individual | Cumulative | Individual |
| Supported order at Receiving end | – | In-order delivery only | Out-of-order delivery as well |

| PROPERTIES | STOP AND WAIT | GO BACK N | SELECTIVE REPEAT |
|---|---|---|---|
| Number of retransmissions in case of packet drop | 1 | N | 1 |

Where,

a = Ratio of Propagation delay and Transmission delay,

At N=1, Go Back N is effectively reduced to Stop and Wait,/li>

As Go Back N acknowledges the packed cumulatively, it rejects out-of-order packets,

As Selective Repeat supports receiving out-of-order packets (it sorts the window after receiving the packets), it uses Independent Acknowledgement to acknowledge the packets.

### 25. Error Detection in Computer Networks

**Error:**
A condition when the receiver's information does not match with the sender's information. During transmission, digital signals suffer from noise that can introduce errors in the binary bits travelling from sender to receiver. That means a 0 bit may change to 1 or a 1 bit may change to 0.

**Error Detecting Codes (Implemented either at Data link layer or Transport Layer of OSI Model)**
Whenever a message is transmitted, it may get scrambled by noise or data may get corrupted. To avoid this, we use error-detecting codes which are additional data added to a given digital message to help us detect if any error has occurred during transmission of the message.

Basic approach used for error detection is the use of redundancy bits, where additional bits are added to facilitate detection of errors.

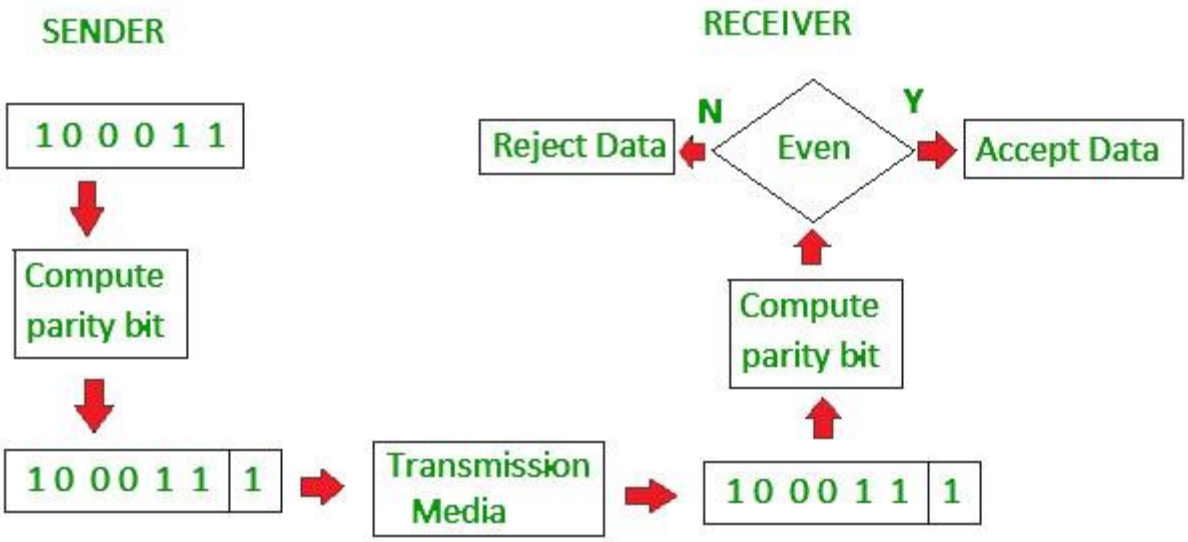
Some popular techniques for error detection are:
1. Simple Parity check
2. Two-dimensional Parity check
3. Checksum
4. Cyclic redundancy check

1. Simple Parity check
Blocks of data from the source are subjected to a check bit or parity bit generator form, where a parity of :

1 is added to the block if it contains odd number of 1's, and

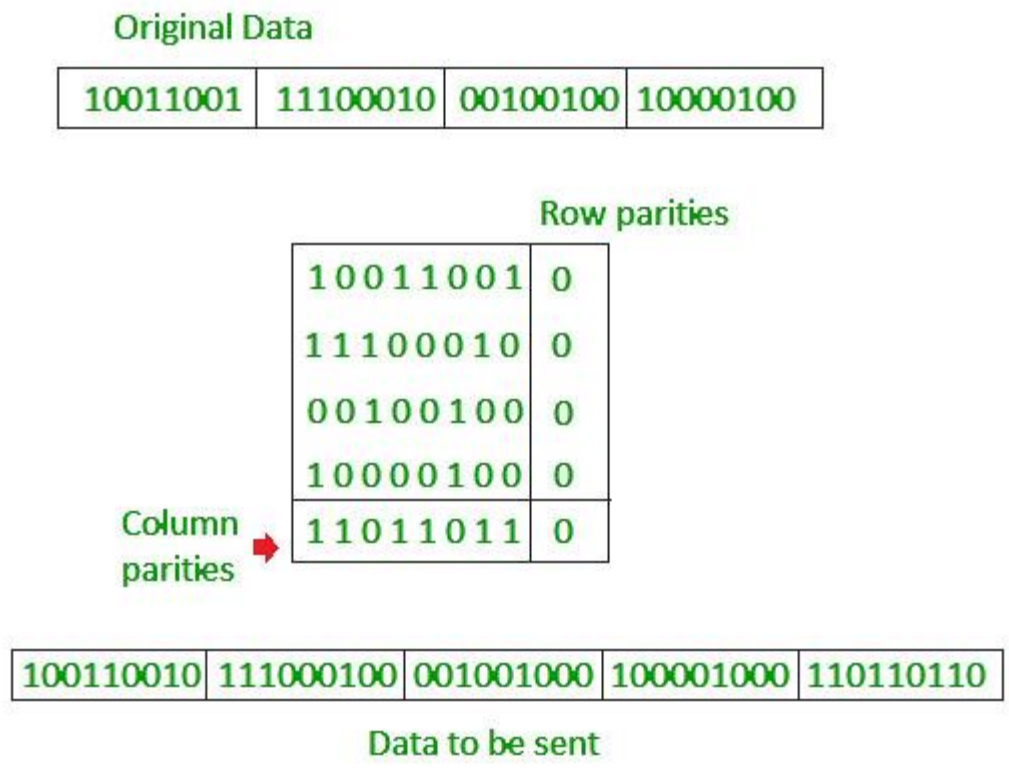
0 is added if it contains even number of 1's

This scheme makes the total number of 1's even, that is why it is called even parity checking.




2. Two-dimensional Parity check

Parity check bits are calculated for each row, which is equivalent to a simple parity check bit. Parity check bits are also calculated for all columns, then both are sent along with the data. At the receiving end these are compared with the parity bits calculated on the received data.




3. Checksum

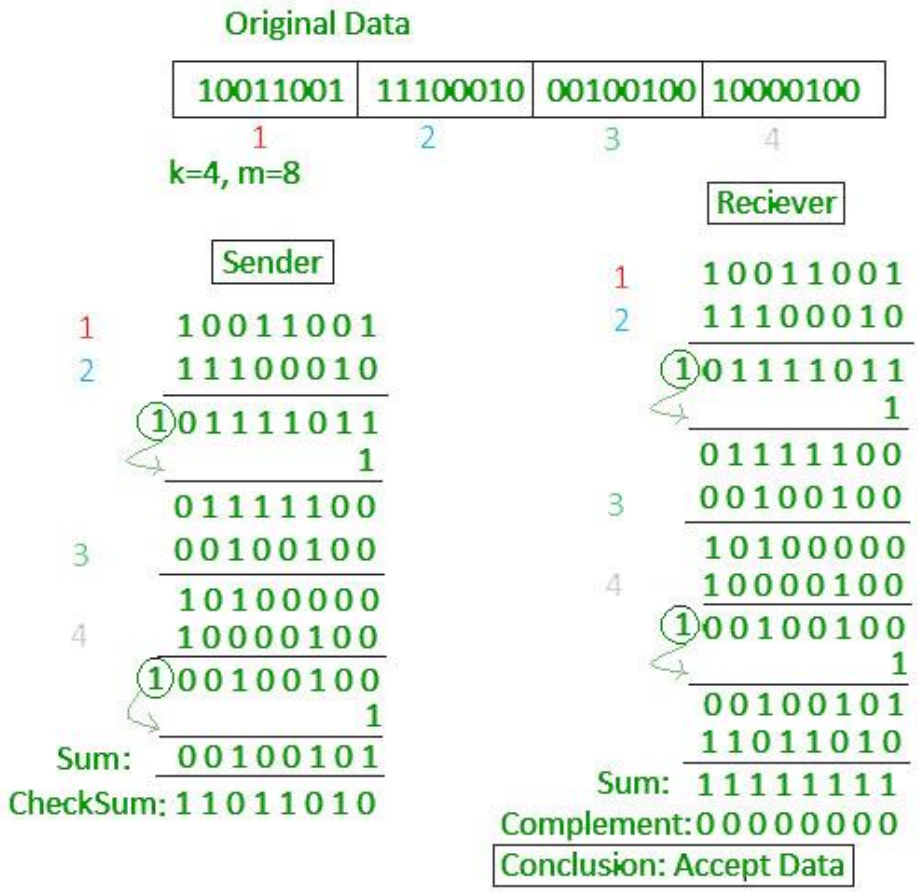
In checksum error detection scheme, the data is divided into k segments each of m bits.

In the sender's end the segments are added using 1's complement arithmetic to get the sum. The sum is complemented to get the checksum.

The checksum segment is sent along with the data segments.

At the receiver's end, all received segments are added using 1's complement arithmetic to get the sum. The sum is complemented.

If the result is zero, the received data is accepted; otherwise discarded.



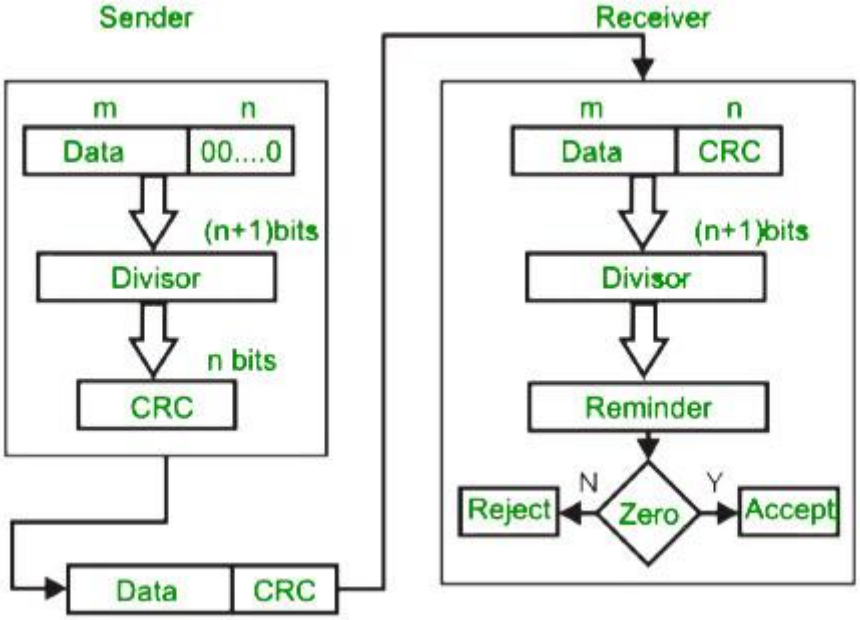

4. Cyclic redundancy check (CRC)

Unlike checksum scheme, which is based on addition, CRC is based on binary division.

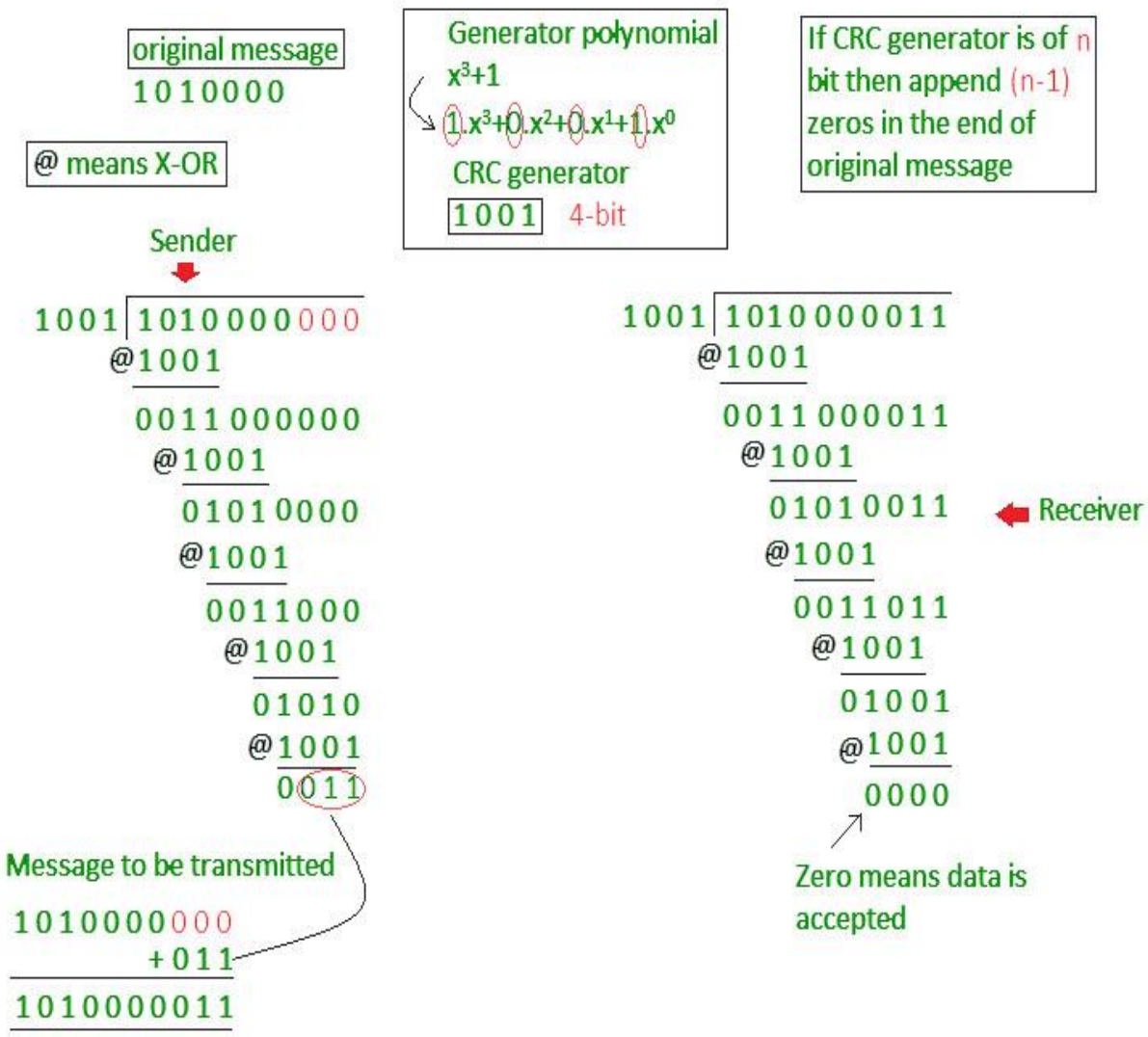
In CRC, a sequence of redundant bits, called cyclic redundancy check bits, are appended to the end of data unit so that the resulting data unit becomes exactly divisible by a second, predetermined binary number.

At the destination, the incoming data unit is divided by the same number. If at this step there is no remainder, the data unit is assumed to be correct and is therefore accepted.

A remainder indicates that the data unit has been damaged in transit and therefore must be rejected.


Sender
Receiver
m
n
Data
00....0
(n+1)bits
Divisor
n bits
CRC
Data
CRC
m
n
Data
CRC
(n+1)bits
Divisor
Reminder
N
Y
Reject
Zero
Accept

Example :




**26. Hamming Code in Computer Network**

Hamming code is a set of error-correction codes that can be used to **detect and correct the errors** that can occur when the data is moved or stored from the sender to the receiver. It is **technique developed by R.W. Hamming for error correction**.

**Redundant bits –**

Redundant bits are extra binary bits that are generated and added to the information-carrying bits of data transfer to ensure that no bits were lost during the data transfer.
The number of redundant bits can be calculated using the following formula:

$2^r \geq m + r + 1$

where, r = redundant bit, m = data bit

Suppose the number of data bits is 7, then the number of redundant bits can be calculated using:
= 2^4 ≥ 7 + 4 + 1
Thus, the number of redundant bits= 4

**Parity bits –**
A parity bit is a bit appended to a data of binary bits to ensure that the total number of 1's in the data is even or odd. Parity bits are used for error detection. There are two types of parity bits:

**Even parity bit:**
In the case of even parity, for a given set of bits, the number of 1's are counted. If that count is odd, the parity bit value is set to 1, making the total count of occurrences of 1's an even number. If the total number of 1's in a given set of bits is already even, the parity bit's value is 0.

**Odd Parity bit –**
In the case of odd parity, for a given set of bits, the number of 1's are counted. If that count is even, the parity bit value is set to 1, making the total count of occurrences of 1's an odd number. If the total number of 1's in a given set of bits is already odd, the parity bit's value is 0.

**General Algorithm of Hamming code –**
The Hamming Code is simply the use of extra parity bits to allow the identification of an error.

Write the bit positions starting from 1 in binary form (1, 10, 11, 100, etc).

All the bit positions that are a power of 2 are marked as parity bits (1, 2, 4, 8, etc).

All the other bit positions are marked as data bits.

Each data bit is included in a unique set of parity bits, as determined its bit position in binary form.
a. Parity bit 1 covers all the bits positions whose binary representation includes a 1 in the least significant position (1, 3, 5, 7, 9, 11, etc).
b. Parity bit 2 covers all the bits positions whose binary representation includes a 1 in the second position from the least significant bit (2, 3, 6, 7, 10, 11, etc).
c. Parity bit 4 covers all the bits positions whose binary representation includes a 1 in the third position from the least significant bit (4–7, 12–15, 20–23, etc).
d. Parity bit 8 covers all the bits positions whose binary representation includes a 1 in the fourth position from the least significant bit bits (8–15, 24–31, 40–47, etc).
e. In general, each parity bit covers all bits where the bitwise AND of the parity position and the bit position is non-zero.

Since we check for even parity set a parity bit to 1 if the total number of ones in the positions it checks is odd.

Set a parity bit to 0 if the total number of ones in the positions it checks is even.

| Position | R8 | R4 | R2 | R1 |
|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 0 | 0 | 1 |
| 2 | 0 | 0 | 1 | 0 |
| 3 | 0 | 0 | 1 | 1 |
| 4 | 0 | 1 | 0 | 0 |
| 5 | 0 | 1 | 0 | 1 |
| 6 | 0 | 1 | 1 | 0 |
| 7 | 0 | 1 | 1 | 1 |
| 8 | 1 | 0 | 0 | 0 |
| 9 | 1 | 0 | 0 | 1 |
| 10 | 1 | 0 | 1 | 0 |
| 11 | 1 | 0 | 1 | 1 |

R1 -> 1,3,5,7,9,11
R2 -> 2,3,6,7,10,11
R3 -> 4,5,6,7
R4 -> 8,9,10,11

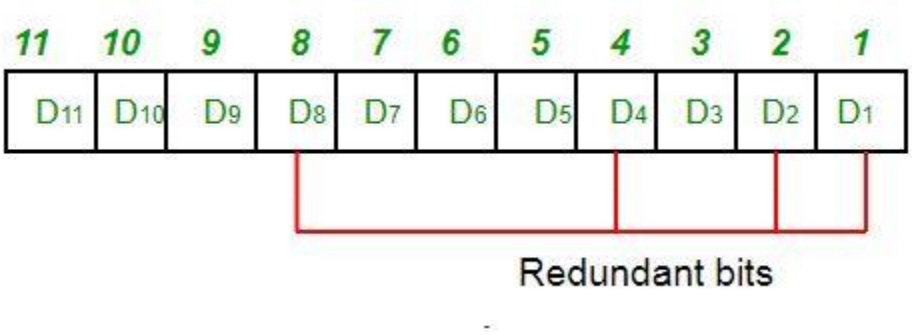
**Determining the position of redundant bits –**
These redundancy bits are placed at the positions which correspond to the power of 2.
As in the above example:

The number of data bits = 7

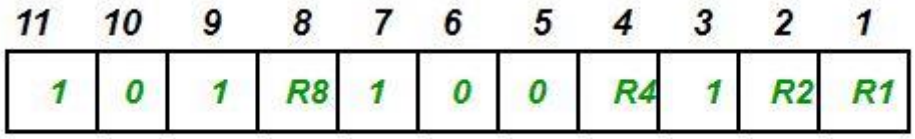
The number of redundant bits = 4

The total number of bits = 11

The redundant bits are placed at positions corresponding to power of 2- 1, 2, 4, and 8



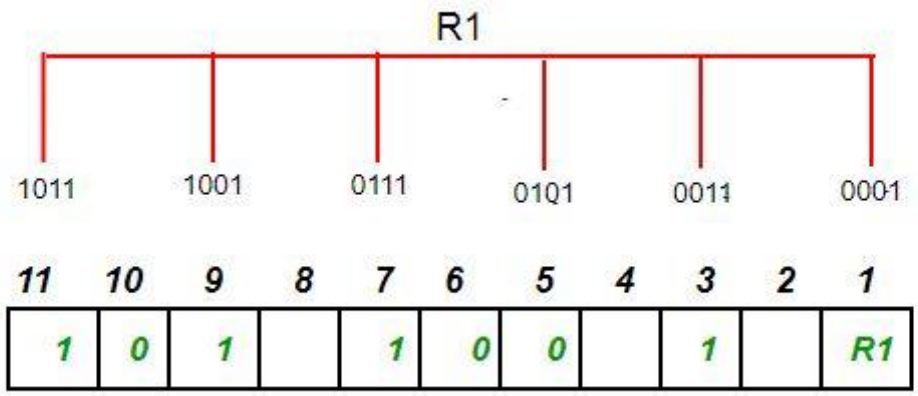

Suppose the data to be transmitted is 1011001, the bits will be placed as follows:




**Determining the Parity bits –**

R1 bit is calculated using parity check at all the bits positions whose binary representation includes a 1 in the least significant position.

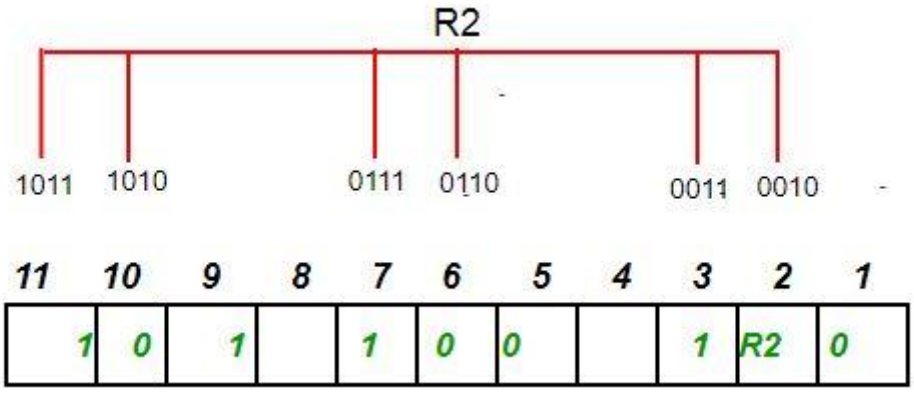
R1: bits 1, 3, 5, 7, 9, 11




To find the redundant bit R1, we check for even parity. Since the total number of 1's in all the bit positions corresponding to R1 is an even number the value of R1 (parity bit's value) = 0

R2 bit is calculated using parity check at all the bits positions whose binary representation includes a 1 in the second position from the least significant bit.

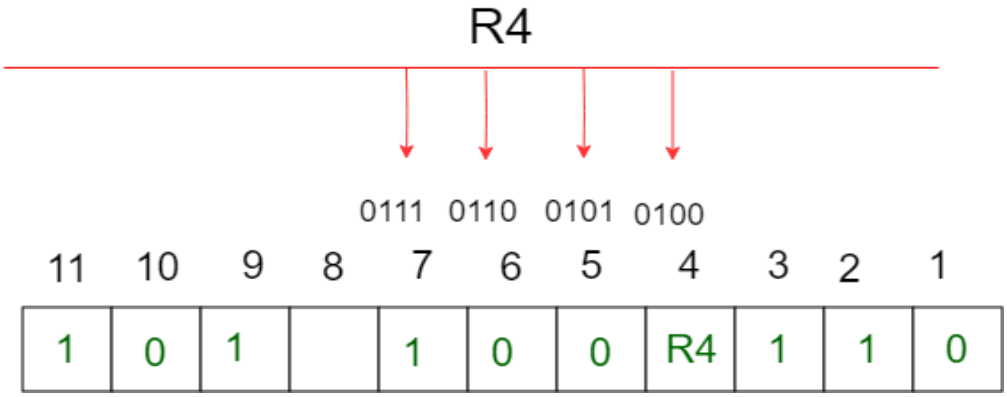
R2: bits 2,3,6,7,10,11




To find the redundant bit R2, we check for even parity. Since the total number of 1's in all the bit positions corresponding to R2 is odd the value of R2(parity bit's value)=1

R4 bit is calculated using parity check at all the bits positions whose binary representation includes a 1 in the third position from the least significant bit.

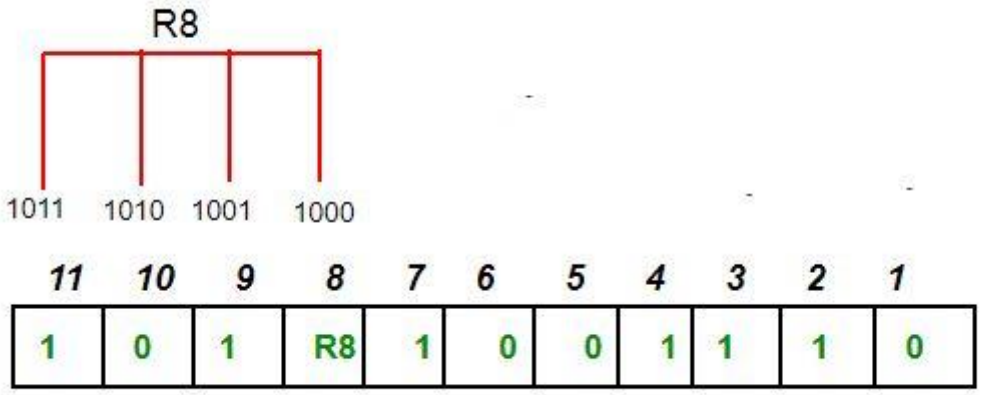
R4: bits 4, 5, 6, 7




To find the redundant bit R4, we check for even parity. Since the total number of 1's in all the bit positions corresponding to R4 is odd the value of R4(parity bit's value) = 1

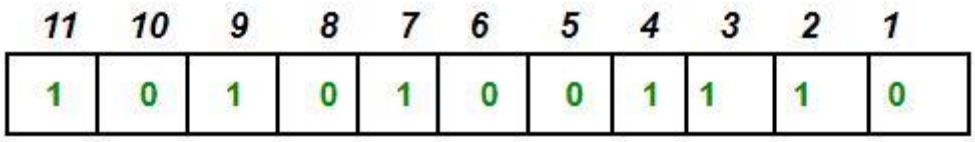
R8 bit is calculated using parity check at all the bits positions whose binary representation includes a 1 in the fourth position from the least significant bit.

R8: bit 8,9,10,11

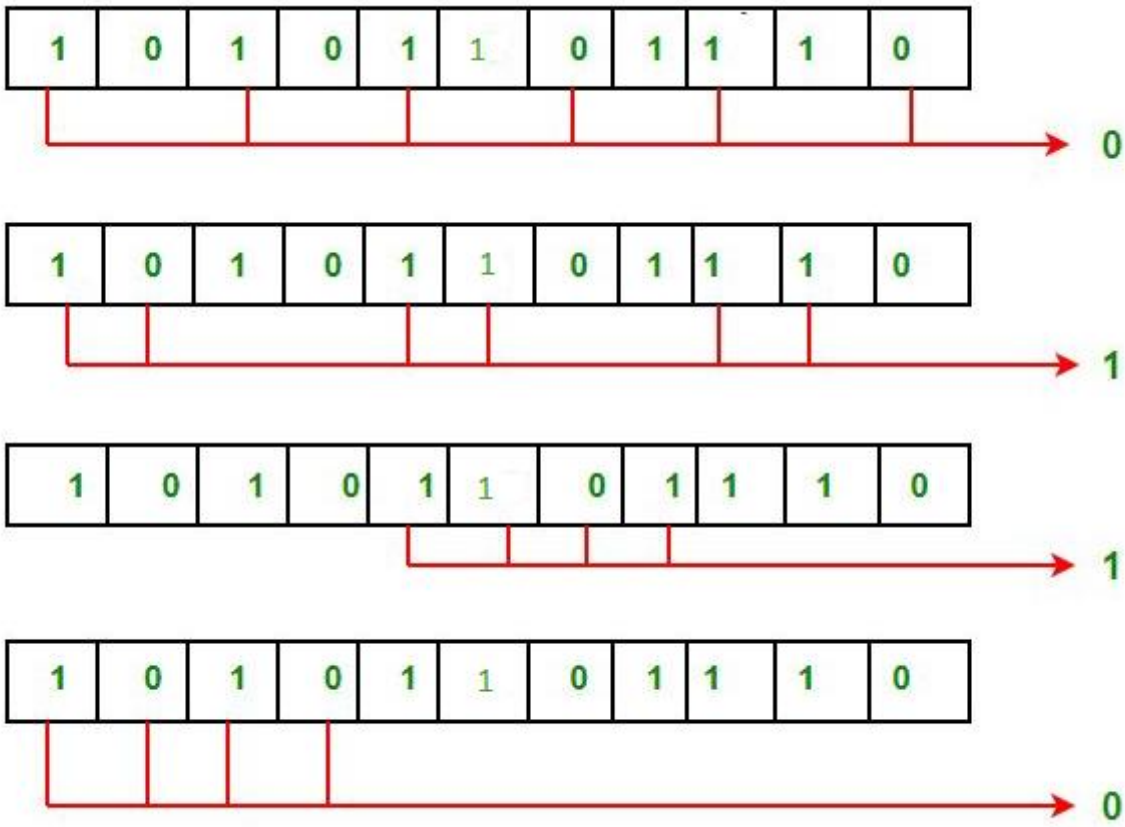


To find the redundant bit R8, we check for even parity. Since the total number of 1's in all the bit positions corresponding to R8 is an even number the value of R8(parity bit's value)=0.

Thus, the data transferred is:




**Error detection and correction –**
Suppose in the above example the 6th bit is changed from 0 to 1 during data transmission, then it gives new parity values in the binary number:

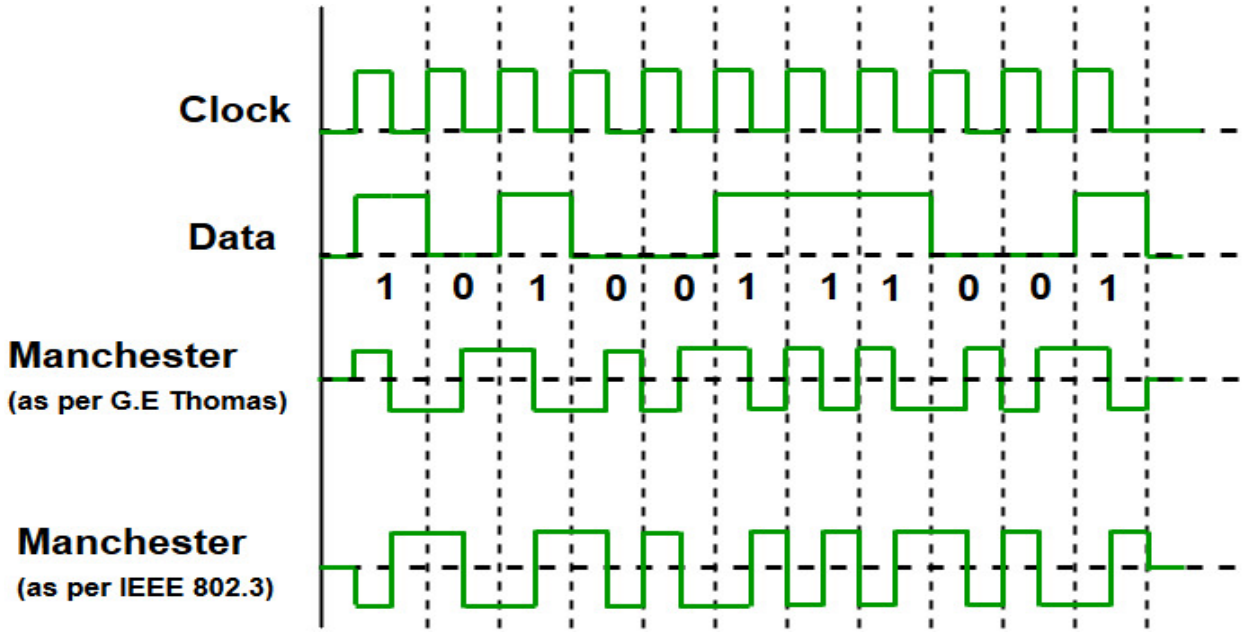



‘

The bits give the binary number as 0110 whose decimal representation is 6. Thus, the bit 6 contains an error. To correct the error the 6th bit is changed from 1 to 0.

**27. Manchester Encoding in Computer Network**

Prerequisite – Difference between Unipolar, Polar and Bipolar Line Coding Schemes
Manchester encoding is a synchronous clock encoding technique used by the physical layer of the Open System Interconnection [OSI] to encode the clock and data of a synchronous bit stream.




The binary data to be transmitted over the cable are not sent as NRZ [Non-return-to-zero].

**Non-return-to-zero [NRZ] –**
NRZ code's voltage level is constant during a bit interval. When there is a long sequence of 0s and 1s, there is a problem at the receiving end. The problem is that the synchronization is lost due to lack of transmissions.
It is of 2 types:

**NRZ-level encoding –**
The polarity of signals changes when incoming signal changes from '1' to '0' or from '0' to '1'. It considers the first bit data as polarity change.

**NRZ-Inverted/ Differential encoding –**
In this, the transitions at the beginning of bit interval is equal to 1 and if there is no transition at the beginning of bit interval is equal to 0.

**Characteristics of Manchester Encoding –**

A logic 0 is indicated by a 0 to 1 transition at the centre of the bit and logic 1 by 1 to 0 transition.

The signal transitions do not always occur at the 'bit boundary' but there is always a transition at the centre of each bit.

The **Differential Physical Layer Transmission** do not employ an inverting line driver to convert the binary digits into an electrical signal. And therefore the signal on the wire is not opposite the output by encoder.

The Manchester Encoding is also called **Biphase code** as each bit is encoded by a positive 90 degrees phase transition or by negative 90 degress phase transiton..

The **Digital Phase Locked Loop (DPLL)** extracts the clock signal and deallocates the value and timming of each bit. The transmitted bit stream must contain a high density of bit transitions.

The Manchester Encoding consumes twice the bandwidth of the original signal.

The advantages of Manchester code is that the DC component of the signal carries no information. This makes it possible that standards that usually do not carry power can transmit this information.

Eg: For 10Mbps LAN the signal spectrum lies between 5 and 20

Another example to find out the bits by seeing the transitions.