Computer Network

A computer network is a set of computers connected together for the purpose of sharing resources. The most common resource shared today is connection to the Internet. Other shared resources can include a printer or a file server. The Internet itself can be considered as a computer network.

Computer network is an interconnection of two or more systems. To interconnect we need a set of wires and set of rules. The set of rules is known as **protocol**

OSI model is a software which convert our data into network presentable format. Like C, is a procedural oriented language and C++ is an object oriented language in a similar way network is a layered structure approach.

In layered structure approach we assign different job to different layer of OSI -layer.

- ISO model is an theoretical concepts.

ISO model consist of seven different layers each layer performs different task.

Application layer
Presentation layer
Session layer
Transport layer
Network layer
Data-link layer
Physical layer

At sender end

Application layer:

Application layer decides data to be transmit. Application layer is a user-interface layer like we use internet by using browser that browser lies in the category of application layer.

In other words, application layer interacts with the end user.

Presentation layer

At Sender End Presentation Layer converts our system data into network presentable form.

For example, conversion of Uni-code to Ascii code is performed at presentation layer.

Optional task of presentation layer

- Data compression
- Data encryption

Session layer

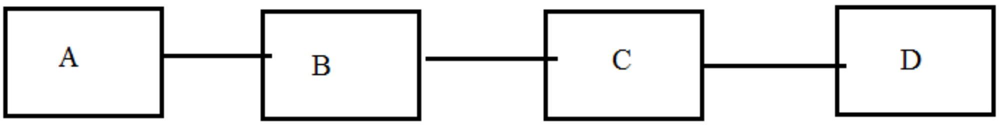
Session layer only maintains the session dialog.

The session layer manages a session by initiating the opening and closing of sessions between end-user application processes. This layer also controls single or multiple connections for each end-user application, and directly communicates with both the presentation and the transport layers. The services offered by the session layer are generally implemented in application environments using remote procedure calls (RPCs).

Transport layer

In Network we do not transmit whole file in a single transmission we divide the file into number of parts then we transmit. The first division of data is performed at transport layer (at sender side). Transport layer divides the data in the form of segments.

If transport layer divides the data into segments, then what will be the size of segments??



Suppose A wants to send data to system D Then B and C are intermediate system. The data of A is first transmitting to B Then B sent to C Then C to D. Now transport layer of system A will communicate with transport layer of system D that what should be the segment size.

Then what should be the criteria of segment size? Segment size = min (Buffer of A, buffer of B). Size of segment is decided by ultimate host and ultimate destination system.

- Transport layer also perform error control and flow control.

Network is responsible for transmission of data from one device to another device. The end to end transfer of data from a transmitting application to a receiving application involves many steps, each subject to error. With the error control process, we can be confident that the transmitted and received data are identical. Data can be corrupted during transmission. For reliable communication, error must be detected and corrected. This process of detecting and correcting error is error control.

Flow control means to overcome mismatch in speed of sender and receiver.

In Communication, there is communication medium between sender and receiver. When Sender sends data to receiver than there can be problem in below case:

1) Sender sends data at higher rate and receive is too sluggish to support that data rate.

To solve the above problem, FLOW CONTROL is introduced. It also works on several higher layers. The main concept of Flow Control is to introduce EFFICIENCY in Computer Networks

Network layer:

Network layer further divides the segment in the form of packets (data-gram). Now why this layer further divides segments into packets??

For example

If we have a segment of size =100kb and bandwidth we have 56kbps. Now this segment cannot be put into the channel, to overcome this problem packets are created. The size of packet is justifying by observing underlining capacity of a channel. This underling capacity of a channel is known as bandwidth.

Function of Network Layer:

Routing

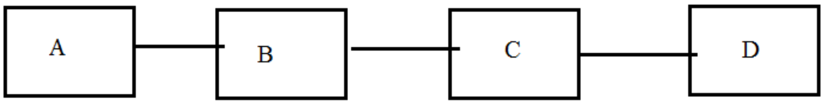
Routing means if there is multi-route to send data from A to B system, this decision will be taken at network layer.

Congestion control

It is the reduced quality of service that occurs when a network node is carrying more data that it can handle.

Data link layer

Data link layer further divides the data into frames. To divide the packet into frames that term is known as **framing**. Data link layer as name suggested it works our a single link.



Flow control

There is a difference between flow control of transport layer and flow control of data link layer.

Responsibility of system A’s data link layer is that the data is successfully reached to system B or not.

But responsibility of transport layer of system A is that data is successfully reached to system D or not.

Error control

Data link layer divides the packets into frames because to keep unit of retransmission very small if any error come.

Physical layer

Physical layer converts the data into voltage level form. Like we send data it travels either through wires or in the air in both case no of bits of data converts into wave forms.

OSI (Open-System-Interconnection) model is called layer to layer or peer to peer protocol.

TCP/IP Protocol

TCP/IP stands for Transfer Control Protocol or Transmission control protocol. **TCP/IP** is open -source software. It is basically four layer model.

Application layer
Transport layer
IP Layer
Host to Network Layer

- **TCP/IP** model is practically used because it came first.
- OSI model is only a theoretical concept by following it we can design new protocol

Some term ology related to Network:

- **Connection oriented network and connection less network.**

  Connection oriented service means before transmission of data we decide from which path that data will flow in the network from sender to receiver end, then data will send by following that path.

  Circuit switching word is also used for connection-oriented service.

  Circuit switch is a special case of connection oriented service. But every connection-oriented service is not necessary circuit switch. Telephone service is an example of circuit switch.

  In circuit switching one physical path will be fixed form sender to receiver connectionless means there is no pre define path exist.

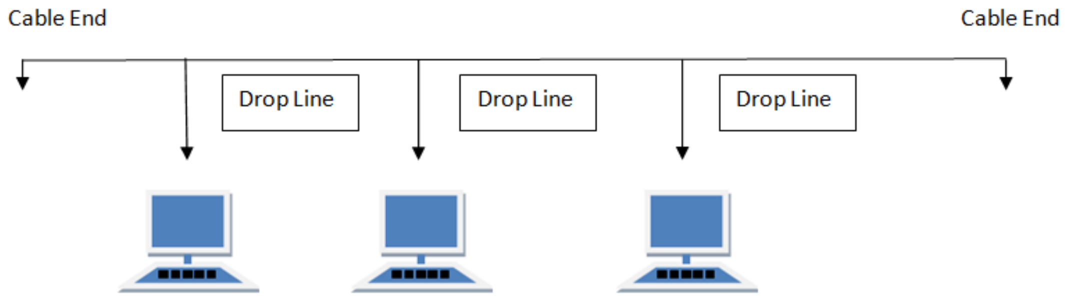
- In connection less there is no guarantee of ordering of data.
- Connectionless service is faster than connection oriented service.
- One of the example of connection-less is packet switched network.
- Ethernet and ATM are packet-switched based network.

Network topology

Network Topology is the schematic description of a network arrangement, connecting various nodes (sender and receiver) through lines of connection.

BUS Topology

Bus topology is a network type in which every computer and network device is connected to single cable. When it has exactly two endpoints, then it is called **Linear Bus topology**.



Features of Bus Topology

1. Every device is connected to a single cable

Advantages of Bus Topology

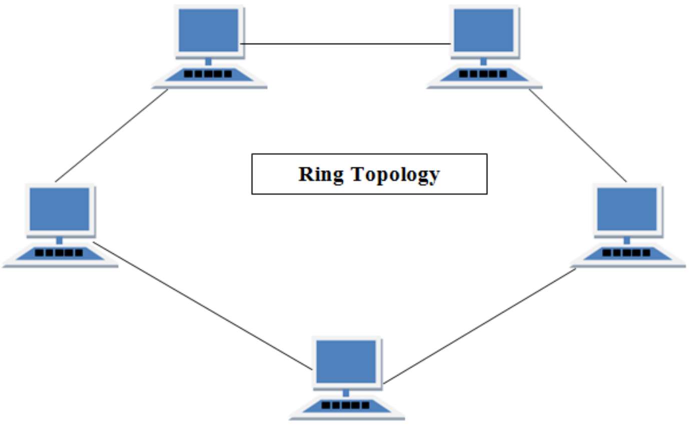
1. It is cost effective.
2. Cable required is least compared to other network topology.
3. Used in small networks.
4. It is easy to understand.
5. Easy to expand joining two cables together.

Disadvantages of Bus Topology

1. Cables fails then whole network fails.
2. If network traffic is heavy or nodes are more the performance of the network decreases.
3. Cable has a limited length.
4. It is slower than the ring topology.

RING Topology

It is called ring topology because it forms a ring as each computer is connected to another computer, with the last one connected to the first. Exactly two neighbors for each device.



Features of Ring Topology

1. A number of repeaters are used for Ring topology with large number of nodes, because if someone wants to send some data to the last node in the ring topology with 100 nodes, then the data will have to pass through 99 nodes to reach the 100th node. Hence to prevent data loss repeaters are used in the network.
2. The transmission is unidirectional, but it can be made bidirectional by having 2 connections between each Network Node, it is called **Dual Ring Topology**.
3. In Dual Ring Topology, two ring networks are formed, and data flow is in opposite direction in them. Also, if one ring fails, the second ring can act as a backup, to keep the network up.
4. Data is transferred in a sequential manner that is bit by bit. Data transmitted, has to pass through each node of the network, till the destination node.

Advantages of Ring Topology

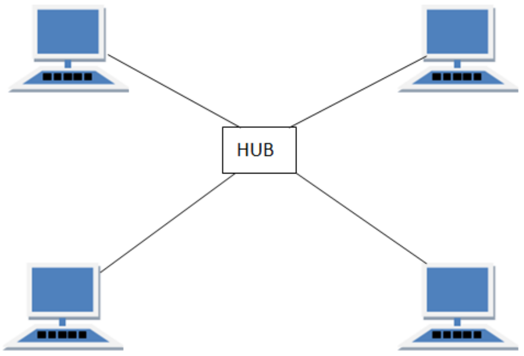
1. Cheap to install and expand

Disadvantages of Ring Topology

1. Troubleshooting is difficult in ring topology.
2. Adding or deleting the computers disturbs the network activity.
3. Failure of one computer disturbs the whole network.

STAR Topology

In this type of topology all the computers are connected to a single hub through a cable. This hub is the central node and all others nodes are connected to the central node.



Features of Star Topology

1. Every node has its own dedicated connection to the hub.
2. Hub acts as a repeater for data flow.
3. Can be used with twisted pair, Optical Fiber or coaxial cable.

Advantages of Star Topology

1. Fast performance with few nodes and low network traffic.
2. Easy to troubleshoot.
3. Easy to setup and modify.
4. Only that node is affected which has failed, rest of the nodes can work smoothly.

Disadvantages of Star Topology

1. Cost of installation is high.
2. Expensive to use.
3. If the hub fails, then the whole network is stopped because all the nodes depend on the hub.
4. Performance is based on the hub that is it depends on its capacity

MESH Topology

It is a point-to-point connection to other nodes or devices. All the network nodes are connected to each other. Mesh has n(n-2)/2 physical channels to link n devices.

There are two techniques to transmit data over the Mesh topology, they are:

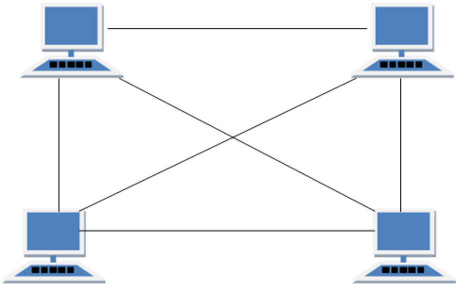
1. Routing
2. Flooding

Routing

In routing, the nodes have a routing logic, as per the network requirements. Like routing logic to direct the data to reach the destination using the shortest distance. Or, routing logic which has information about the broken links, and it avoids those node etc. We can even have routing logic, to re-configure the failed nodes.

Flooding

In flooding, the same data is transmitted to all the network nodes, hence no routing logic is required. The network is robust, and the its very unlikely to lose the data. But it leads to unwanted load over the network.



Types of Mesh Topology

1. **Partial Mesh Topology:**

   In this topology some of the systems are connected in the same fashion as mesh topology but some devices are only connected to two or three devices.

2. **Full Mesh Topology**

   Each and every nodes or devices are connected to each other.

Features of Mesh Topology

1. Fully connected.
2. Robust.

Advantages of Mesh Topology

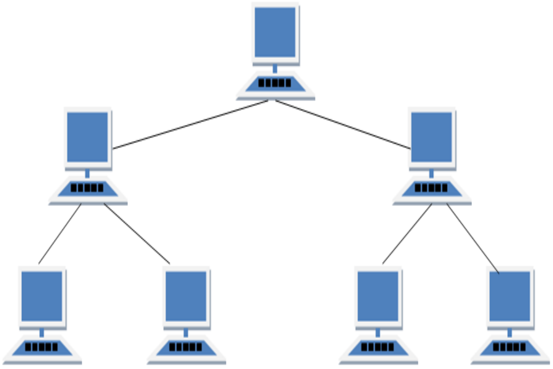
1. Each connection can carry its own data load.
2. It is robust.
3. Fault is diagnosed easily.

Disadvantages of Mesh Topology

1. Installation and configuration is difficult.
2. Cabling cost is more.
3. Bulk wiring is required.

TREE Topology

It has a root node and all other nodes are connected to it forming a hierarchy. It is also called hierarchical topology. It should at least have three levels to the hierarchy.



Features of Tree Topology

1. Ideal if workstations are located in groups.
2. Used in Wide Area Network.

Advantages of Tree Topology

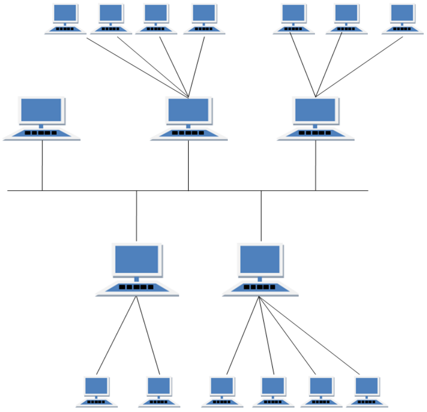
1. Extension of bus and star topologies.
2. Expansion of nodes is possible and easy.
3. Easily managed and maintained.
4. Error detection is easily done.

Disadvantages of Tree Topology

1. Heavily cabled.
2. Costly.
3. If more nodes are added maintenance is difficult.
4. Central hub fails, network fails.

HYBRID Topology

It is two different types of topologies which is a mixture of two or more topologies. For example, if in an office in one department ring topology is used and in another star topology is used, connecting these topologies will result in Hybrid Topology (ring topology and star topology).



Features of Hybrid Topology

1. It is a combination of two or topologies
2. Inherits the advantages and disadvantages of the topologies included

Advantages of Hybrid Topology

1. Reliable as Error detecting and troubleshooting is easy.
2. Effective.
3. Scalable as size can be increased easily.
4. Flexible.

Disadvantages of Hybrid Topology

1. Complex in design.
2. Costly.

Reliable network

If your network is reliable then sender ensures that whether the receiver receives the data correctly or not

Data link layer:

Responsibility of data link layer are:

- Framing
- Error control
- Flow control

Framing

How receiver decides frame boundary?

First of all, why receiver have to decide frame boundary?? Because error control is done by receiver on only one frame.

Solution

- Fix the length of frames.

Example

First 100 bytes is of first frame and next 100 bytes for next and so on. But in this case we also have a problem that we have to send minimum data of 100 bytes. If data is less than 100 bytes, then what to do? So this solution is not practically feasible.

- Specify the frame length in frame header
- Character stuffing

  In the second method, each frame starts with the ASCII character sequence DLE STX and ends with the sequence DLE ETX. (where DLE is Data Link Escape, STX is Start of TeXt and ETX is End of TeXt.) This method overcomes the drawbacks of the character count method. If the destination ever loses synchronization, it only has to look for DLE STX and DLE ETX characters. If, however, binary data is being transmitted then there exists a possibility of the characters DLE STX and DLE ETX occurring in the data. Since this can interfere with the framing, a technique called character stuffing is used. The sender's data link layer inserts an ASCII DLE character just before the DLE character in the data. The receiver's data link layer removes this DLE before this data is given to the network layer. However, character stuffing is closely associated with 8-bit characters and this is a major hurdle in transmitting arbitrary sized characters.

- **Bit stuffing**

The third method allows data frames to contain an arbitrary number of bits and allows character codes with an arbitrary number of bits per character. At the start and end of each frame is a flag byte consisting of the special bit pattern 01111110. Whenever the sender's data link layer encounters five consecutive 1s in the data, it automatically stuffs a zero bit into the outgoing bit stream. This technique is called bit stuffing. When the receiver sees five consecutive 1s in the incoming data stream, followed by a zero bit, it automatically destuffs the 0 bit. The boundary between two frames can be determined by locating the flag pattern.

- **Error detection**

The bit stream transmitted by the physical layer is not guaranteed to be error free. The data link layer is responsible for error detection and correction. The most common error control method is to compute and append some form of a checksum to each outgoing frame at the sender's data link layer and to recompute the checksum and verify it with the received checksum at the receiver's side. If both of them match, then the frame is correctly received; else it is erroneous. The checksums may be of two types:

- **Error detecting**

  Receiver can only detect the error in the frame and inform the sender about it.

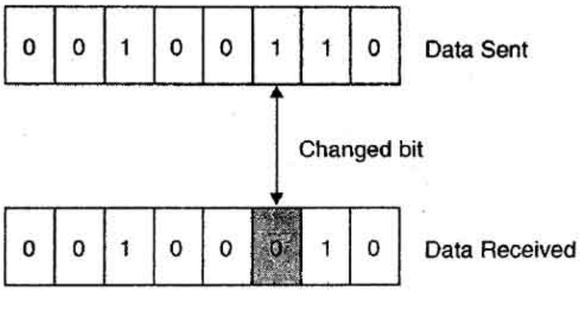
- **Error detecting and correcting**:
  The receiver can not only detect the error but also correct it.

Types of error

- Single bit error
- Multibit error
- Burst error

Single bit error

As name suggest single-bit errors occur when a single bit gets changed during transmission of data due to interference in network communication.



Single bit error

Single-bit errors are least likely type of error because their duration or noise is normally longer than duration of 1 bit.

Multi-bit error

More than on bit is corrupted, very common in serial transmission of data

Transmit bit: 1 0 1 0 1

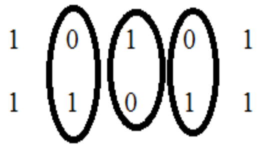
Receiver bit: 1 1 0 1 1

3 bits are corrupted

Burst error

When more than a single bit of data unit gets corrupted (not necessary continuous) it is known as Burst error.

In comparison of single-bit errors, burst errors are more likely to occur. Because as we know that the duration of noise is generally longer than the duration of transferring 1bit, that means with longer duration noise can corrupt more than 1 bit easily. Number of bit affected depends on the data rate and duration of noise.



3 bits burst error

Use of redundancy

Addition bits are added to detection and correct of errors

DATA BIT/MSG BIT	FRAME CHECK SYSTEM(FCS)

Popular techniques used to handle with error

- Simple parity check
- 2-D parity check
- Cyclic redundancy check
- Check sum

Simple parity check

Simple example of error detection technique is parity bit. The parity bit is chosen that the number of 1 bits in the code word is either even(for even parity) or odd (for odd parity).

For example, when 10110101 is transmitted then for even parity an 1 will be appended to the data and for odd parity a 0 will be appended. This scheme can detect only single bits. So if two or more bits are changed then that cannot be detected.

DATA BIT/MSG BIT	Parity Bit

There are two types of parity

1. Odd parity
2. Even parity

Odd parity

Odd parity means odd number of 1's including extra bits.

Even parity

Even parity means even number of 1's including extra bit.

Example

1 0 1 1 0 0 1 0-→ even parity

1 →odd parity

- Simple parity check can detect all single bit error.
- It can also detect burst error if the number of bits in error is odd.

Example:

Here in this Example Parity is even

1 0 1 1	1	**Transmitted Data**
1 0 0 0	1	**Received Data**

- Here we cannot detect even bit burst length error

Second example

1 0 1 1	**1**	**Transmitted Data**
		Error detected
0 0 0 0	**0**	**Received Data**

This technique is not foolproof against burst error that inverts more than one bit. If an even number of bits are inverted due to error, the error is not detected.

2-D parity check(LRC)

- This technique can correct and detect one bit error.
- Performance can be improved by using 2D parity check which organizes the block of bits in the form of table.

- Parity check bit are calculated for each row which is equivalent to simple parity check.
- Parity check bit are also calculated for all columns. Both are send along with the data.

At receiver end they are compared with parity bit.

For example :

Original data we have :

1011011:10101011:01011010:11010101

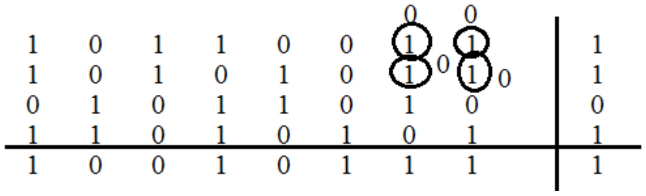
1	0	1	1	0	0	1	1	1
1	0	1	0	1	0	1	1	1
0	1	0	1	1	0	1	0	0
1	1	0	1	0	1	0	1	1
1	1	0	1	0	1	0	1	1
1	0	0	1	0	1	1	1	1

Data to be send :

10110111:10101011:010110100: 110101011:100101111

Performance of 2D Parity check

- Extra overhead is traded for better error detection capability
- 2D parity check significantly improve error detection capability compare to a simple parity check.
- It can detect many burst error but not all.



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

- This error cannot be detected by 2D parity check.

CRC:(**Cyclic Redundancy Checksum)**

An error detection mechanism in which a special number is appended to a block of data in order to detect any changes introduced during storage (or transmission). The CRC is recalculated on retrieval (or reception) and compared to the value originally transmitted, which can reveal certain types of error. For example, a single corrupted bit in the data results in a one-bit change in the calculated CRC, but multiple corrupt bits may cancel each other out.

A CRC is derived using a more complex algorithm than the simple CHECKSUM, involving MODULO ARITHMETIC (hence the 'cyclic' name) and treating each input word as a set of coefficients for a polynomial.

- CRC is more powerful than VRC and LRC in detecting errors.
- It is not based on binary addition like VRC and LRC. Rather it is based on binary division.
- At the sender side, the data unit to be transmitted is divided by a predetermined divisor (binary number) in order to obtain the remainder. This remainder is called **CRC**.
- The CRC has one bit less than the divisor. It means that if CRC is of n bits, divisor is of n+ 1 bit.
- The sender appends this CRC to the end of data unit such that the resulting data unit becomes exactly divisible by predetermined divisor *i.e.* remainder becomes zero.
- At the destination, the incoming data unit *i.e.* data + CRC is divided by the same number (predetermined binary divisor).
- If the remainder after division is zero, then there is no error in the data unit & receiver accepts it.
- If remainder after division is not zero, it indicates that the data unit has been damaged in transit and therefore it is rejected.
- This technique is more powerful than the parity checks and checksum error detection.
- CRC is based on binary division. A sequence of redundant bits called CRC or CRC remainder is appended at the end of a data unit such as byte.

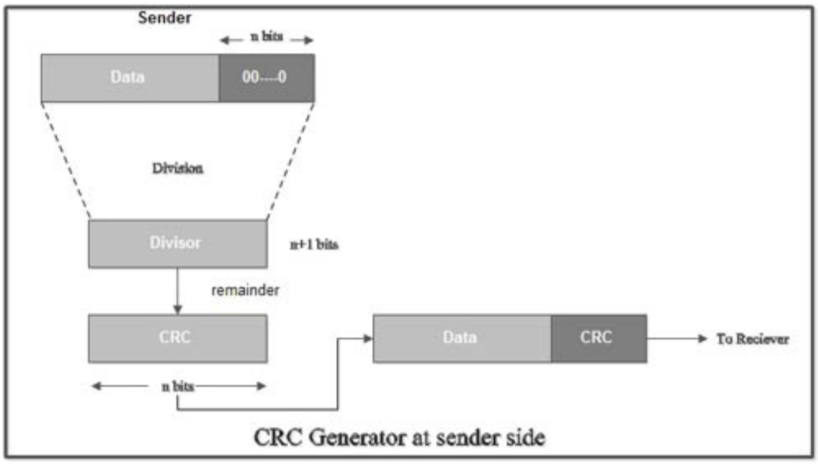
Requirements of CRC:

A CRC will be valid if and only if it satisfies the following requirements:

- It should have exactly one less bit than divisor. Appending the CRC to the end of the data unit should result in the bit sequence which is exactly divisible by the divisor.

The various steps followed in the CRC method are

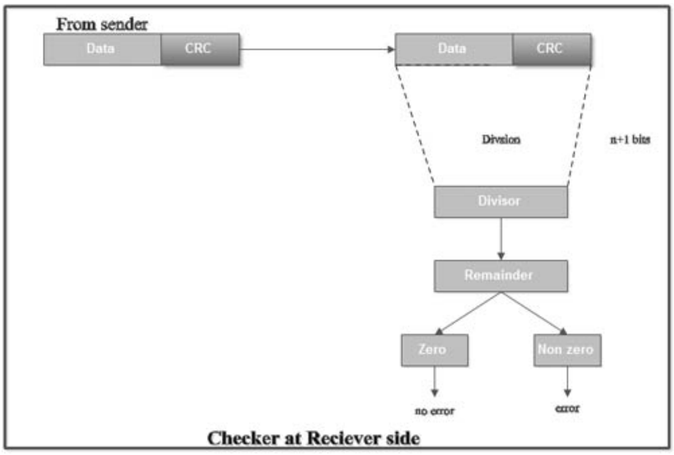
1. A string of n as is appended to the data unit. The length of predetermined divisor is n+ 1.
2. The newly formed data unit *i.e.* original data + string of n as are divided by the divisor using binary division and remainder is obtained. This remainder is called CRC.



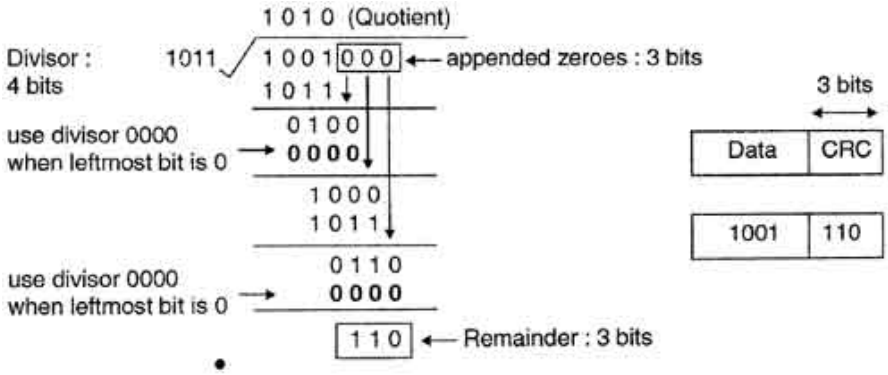
3. Now, string of n O's appended to data unit is replaced by the CRC remainder (which is also of n bit).
4. The data unit + CRC is then transmitted to receiver.
5. The receiver on receiving it divides data unit + CRC by the same divisor & checks the remainder.
6. If the remainder of division is zero, receiver assumes that there is no error in data and it accepts it.
7. If remainder is non-zero, then there is an error in data and receiver rejects it.

- For example, if data to be transmitted is 1001 and predetermined divisor is 1011. The procedure given below is used:

  String of 3 zeroes is appended to 1011 as divisor is of 4 bits. Now newly formed data is 1011000.

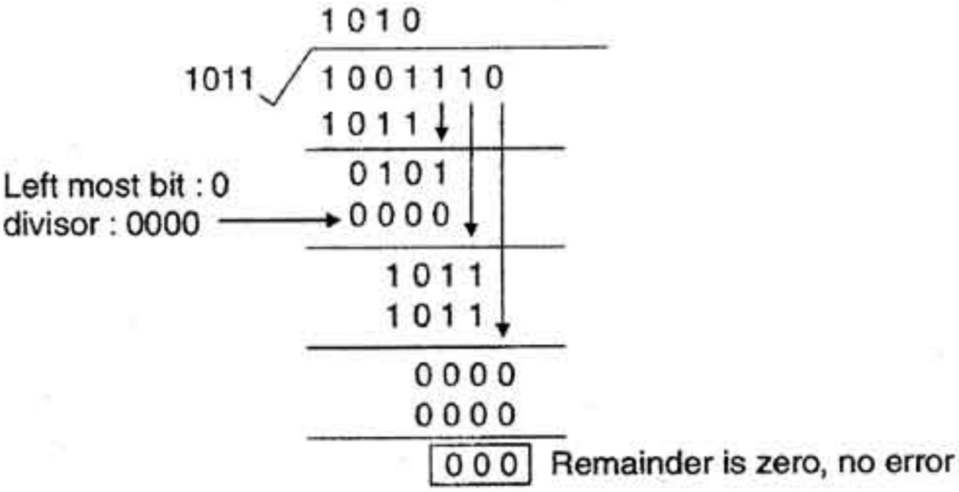


Data unit 1011000 is divided by 1011.



CRC generated (Binary division)

1. During this process of division, whenever the leftmost bit of dividend or remainder is 0, we use a string of Os of same length as divisor. Thus in this case divisor 1011 is replaced by 0000.
2. At the receiver side, data received is 1001110.
3. This data is again divided by a divisor 1011.
4. The remainder obtained is 000; it means there is no error.

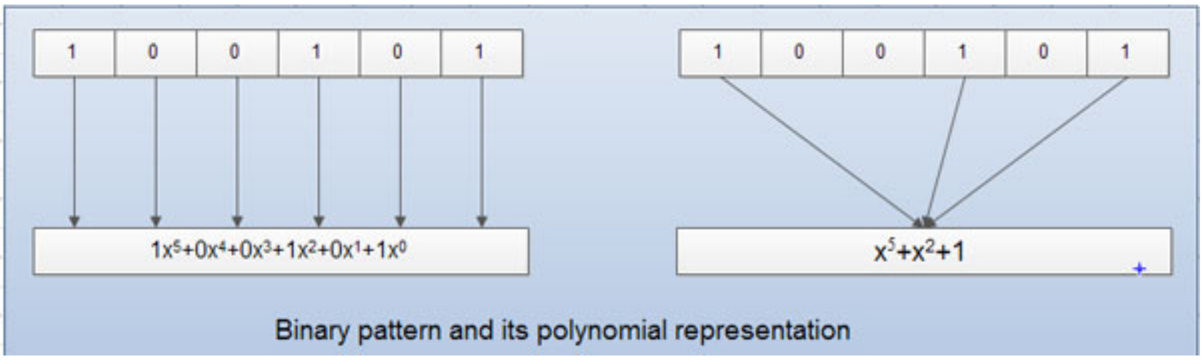


CRC decoded (binary division)

- CRC can detect all the burst errors that affect an odd number of bits.
- The probability of error detection and the types of detectable errors depends on the choice of divisor.
- Thus two major requirement of CRC are:

1. CRC should have exactly one bit less than divisor.

- Appending the CRC to the end of the data unit should result in the bit sequence which is exactly divisible by the divisor.
- **Polynomial codes**
  - A pattern of O's and 1's can be represented as a polynomial with coefficient of o and 1.
  - Here, the power of each term shows the position of the bit and the coefficient shows the values of the bit.
  - For example, if binary pattern is 100101, its corresponding polynomial representation is $x^5 + x^2 + 1$. Figure shows the polynomial where all the terms with zero coefficient are removed and x J is replaced by x and XO by 1.



Binary pattern and its polynomial representation

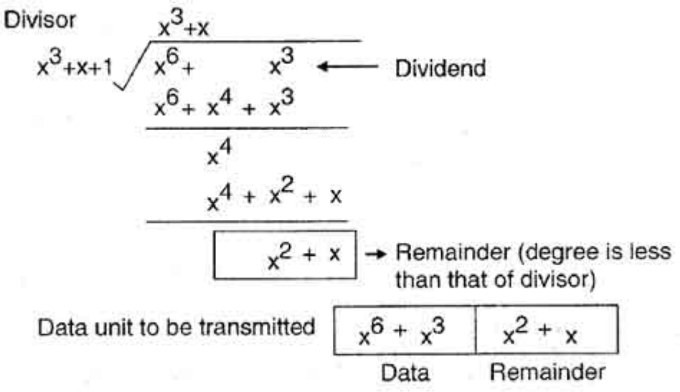
  - The benefits of using polynomial codes is that it produces short codes. For example here a 6-bit pattern is replaced by 3 terms.
  - In polynomial codes, the degree is 1 less than the number of bits in the binary pattern. The degree of polynomial is the highest power in polynomial. For example as shown in fig degree of polynomial $x^5 + x^2 + 1$ are 5. The bit pattern in this case is 6.
  - Addition of two polynomials is based on modulo-2 method. In such as case, addition and subtraction is same.
  - Addition or subtraction is. done by combining terms and deleting pairs of identical terms. For example, adding $x^5 + x^4 + x^2$ and $x^6 + x^4 + x^2$ give $x^6 + x^5$. The terms x^4 and x^2 are deleted.
  - If three polynomials are to be added and if we get a same term three times, a pair of them is detected and the third term is kept. For example, if there is x^2 three times then we keep only one x^2.
  - In case of multiplication of two polynomials, their powers are added. For example, multiplying $x^5 + x^3 + x^2 + x$ with $x^2 + x + 1$ yields:
- $(x^5 + x^3 + x^2 + x)\ (x^2 + x + 1)$

- = $x^7 + x^6 + x^5 + x^5 + x^4 + x^3 + x^4 + x^3 + x^2 + x^3 + x^2 + x$
- =$x^7+x^6+x^3+X$
- In this, first polynomial is multiplied by all terms of second. The result is then simplified and pairs of equal terms are deleted.
  - In case of division, the two polynomials are divided as per the rules of binary division, until the degree of dividend is less than that of divisor.

CRC generator using polynomials

If we consider the data unit 1001 and divisor or polynomial generator 1011their polynomial representation is:

Data	1001	$x^3 + 1$
Division (polynomial generator)	1011	$x^3 + x + 1$



CRC division using polynomial

Now string of n 0s (one less than that of divisor) is appended to data. Now data is 1001000 and its corresponding polynomial representation is $x^6 + x^3$.

The division of x^6+x^3 by x^3+x+1 is shown in fig.

The polynomial generator should have following properties:

1. It should have at least two terms.

2. The coefficient of the term x^0 should be 1.

3. It should not be divisible by x.

4. It should be divisible by x+ 1.

Hamming code:

It is not only detecting error but also correct error.

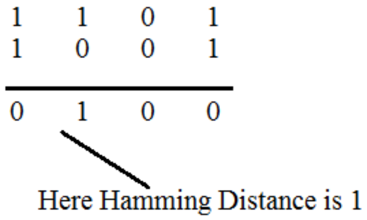
<u>Hamming distance:</u>

Minimum distance between any two code words in a code is called Hamming Distance.

Example:

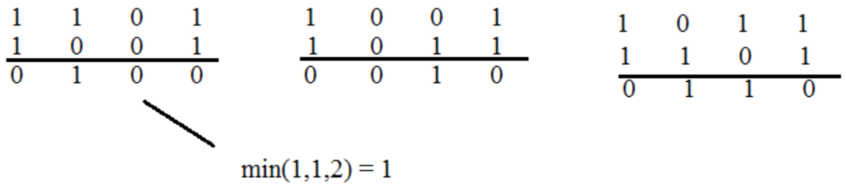
Perform XoR between two code words then count the number of 1's in the result.

Number of 1's will be the hamming distance.



<u>Important point</u>

If we have to find hamming distance between 1101,1001,1011 then



- To detect d bit error then hamming code must be d+1 distance apart.
- To correct d bit error your code should be 2d+1 apart.

If hamming distance of code word is 8 apart then how many bits can be corrected?

Answer:

2d+1=8

2d=7

d=3.5

⇨ 3 bits can be correct

<u>Practically implementation of Hamming code</u>

- It can correct single bit.
- **Number of Reductant bit = Minimum value of r**

d+r+1<=2^r

if d=8 (Length of data)

8+r+1<=2^r

9+r<=2^r

r=4 ➔ satisfied

<u>Working</u>:

Data bit =1011010

d=8 and r=4

1	2	3	4	5	6	7	8	9	10	11	12
2^0	**2^1**		**2^2**				**2^3**				
1	0	1	0	0	0	1	1	1	0	1	0

Redundant bit will be present in the power of 2.

$1=2^0$

$2=2^1$

$3=2^0+2^1$

$4=2^2$

$5=2^0+2^2$

$6=2^2+2^1$

$7=2^2+2^1+2^0$

$8=2^3$

$9=2^3+2^0$

$10=2^3+2^1$

$11=2^0+2^1+2^3$

$12=2^2+2^3$

Consider odd parity: (If in the question it is not mentioned, consider odd parity)

The term 2^0 are appeared in which of the number, numbers are 1,3,5,7,9,11

In that position number of 1's is 4 since it is odd parity therefore at 2^0 there will be one. The term 2^1 are appeared in 2,3,6,7,10,11. Number of 1's is 3 since it is odd parity therefore at 2^1 there will be 0.

Like in this way we will compute 2^2 and 2^3 redundant bit.

- How to correct single bit error by using hamming code

  Let us see previous example:

  Data bit :- 1 0 0 1 0 1 0 1 0

  Data bit with redundant bit 1 0 1 0 0 0 1 1 1 0 1 0

  Suppose 5th bit is corrupted

1 2 3 4 5 6 7 8 9 10 11 12

Corrupted

Taking odd parity into considersion

2^0 : 1,3,5,7,9,11 → 2^0 is corrupted

2^1 : 2,3,6,7,10,11 → 2^1 (no error)

2^2 : 4,5,6,7,12 → 2^2 (corrupted)

2^3 : 8,9,10,11,12 → 2^3 (no error)

Those redundant bit which are corrupted add them

2^0+2^2 = 5th bit is corrupted

Important point:

- Practically hamming code technique is not used
- It is also known as **forward error detection techniques**, means it detect the error and correct it and sender doesn't retransmit the data
- Backward error detection

  When an error is detected in a frame then the sender is asked to retransmit the data/frame. This approach is knowns as automatic report request (**ARQ**) technique

Flow control

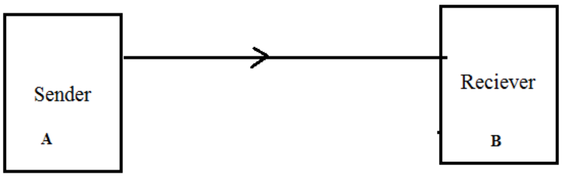
Flow control means to synchronic between sender and receiver

Different types of channel

- Simplex
- Half duplex
- Full-duplex

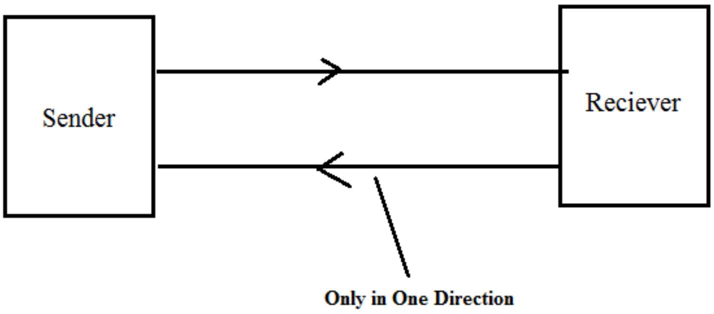
Simplex

Data are send only in one direction. i.e. sender to receiver or receiver to sender



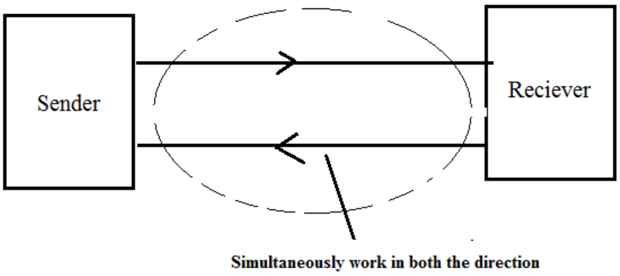
Half duplex

Data are send in both the direction but one at a time.



Full duplex

Data are send in both the direction simultaneously.

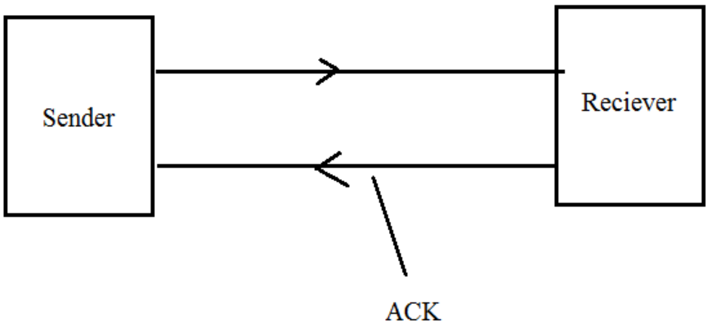


Stop and wait protocol

- This protocol controls the flow control
- In this protocol sender should sent a frame and wait for acknowledgement.
- If in that waiting time we did not get acknowledgement, then sender will be time out for that packet.
- If acknowledgement of first came then only second frame should be send and so on.

How much time we have to wait??

Slightly greater than round-trip time (RTT)



RTT=Data transmit time + acknowledgment time

- How to calculate RTT??

  By using two parameters we can find RTT.

- Transmission time (t_x)
- Propagation time (t_p)

Transmission time

Time taken to put all the bit of data over a media/channel is known as transmission time. It is denoted by t_x.

Propagation time

Time taken by single bit to traverse the distance between sender and receiver, it is denoted by t_p.

$t_x + t_p$ → At this time receiver will receive the data

$t_{p:}$ - Last bit to receive at receiver end

$$RTT= \underset{\substack{\downarrow\\ \text{For Frame}}}{t_x} + t_p + \underset{\substack{\downarrow\\ \text{for Ack}}}{t_{xA}} + t_p + \text{Frame Processing Time}$$

Generally, $RTT= t_x + 2t_p$

Round trip time is the time difference between transmission of first but of data by sender and last bit of acknowledgment is known as RTT

- How to Calculate Transmission time (t_x)

  t_x = length of Data / Data -transfer rate = L/R

- MB→ Mega Bytes
- Mb→ Mega Bits
- Mbps: 10^6 bits per sec
- Kbps : 10^3 bits per sec
- Gbps : 10^9 bits per sec

- Calculation of Propagation Time (t_p)

  t_p = Distance Between Two Station / Signal Propagation Speed

  Speed of light = $3*10^8$

  - Efficiency

    μ = useful time / total time = $t_x/RTT = t_x/ (t_x +2\ t_p)$

Special point

- If length of acknowledgement bit is given, then consider acknowledgment time is also in RTT

- If there is a 2-way Communication, then we do not send acknowledgment separately we include acknowledgement in data bit itself. This concept is known as Piggybacking.

How Receiver distinguish new frame and old frame?

To distinguish this, we use sequence number.

Effective Data Rate/ Throughput /Good put/Channel Utilization

- μ*actual data rate

- Under what condition stop and wait protocol uses the efficiency of 100%

$$\mu = t_x / (t_x + 2\ t_p)$$

$$(t_x + 2\ t_p) = t_x$$

$$t_p = 0$$

  which is not possible to achieve efficiency of 100% in stop and wait protocol therefore, we cannot achieve 100% efficiency in Stop and wait protocol, to run stop and wait problem we need at least half duplex channel.

- If sender continuously send data without waiting for acknowledgement, then we get 100% efficiency. To improve efficiency a new protocol was introduced that is called **sliding window protocol**.

  In sliding window protocol both the sender and receiver decides the window size. If window size is **w,** then sender can send **w** frames without waiting for acknowledgement.

  Efficiency

  $\mu = (w*t_x)/RTT = (w*t_x)/\ (tx + 2\ t_p)$

  If window size is 10 then sender should contain 10 unacknowledgement frame.

  If higher order is send by receiver then it means lower frame all are acknowledged, this concept is called as **cumulative acknowledgement** or **collective acknowledgement**.

  Error

  If in our frame there is some error, then what sliding window protocol will do?

1st condition

We send only one frame in which error has been come. This type of functionality is provided by **Selective Repeat**.

2nd condition

We send all the frames that are present in window if error come in any frame. This type of functionality is provided by **Go-Back-N.**

- Why to use Go-Back N?

  In selective repeat, Buffer at receiver should be equal to at least buffer at sender.

  We should use Go-back N when receiver has window size =1.

Important point

If window size is **w**, then counting of frames start from 0 to w-1 in sliding window protocol.

If w=7 then counting of frames start from 0 to 6.

➔window size =max sequence +1

Number of bits required to store MAX sequence = $\log_2$(Max Sequence +1)

- In selective repeat:

  2w -1 = Max Sequence

  w= (Max Sequence +1)/ 2

- In go back n:

  window size = Max Sequence

question 46 cs-2006

question 44 cs-2006

cs-2009 57 d

cs-2009 58 c

Data link layer is further divided into two sublayers:

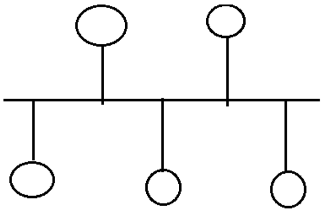
- LLC (logical Link Layer)
- Mac Layer (Medium- Access - Control)
  Mac -layer is particular useful in Lan- Transmission.

There are two addresses stored in our system

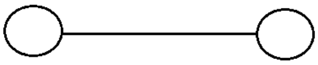
- Mac address (it is the address of Hardware)
- IP address (Logical Address)
- Every system will receive all the frames this type of system is known as broadcasting system.

There exist two types of links

- Broadcast link
- Point to point link



BroadCast- Link

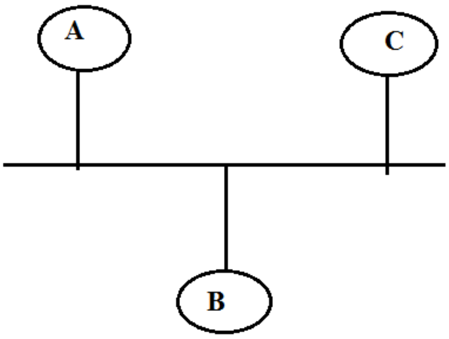


Point to Point Link

Access control protocol

Access control protocol is used to decide which system should transmit and for how much time it will transmit. First access control protocol we are discussing it is **CSMA**

Consider the following situation: -



Consider the following situation

A system wants to send data to system C at the same time C also want to send data to B. Now A also put data on channel and C also put data on channel due to this collision will occur, both the frame will be colliding.

How to avoid this collision

- To avoid this collision many protocol is there which work at Mac Layer.

  We discussing one of them **CSMA**

- CSMA stands for **C**arrier **S**ensing **M**ultiple **A**ccess **P**oint **P**rotocol
- Carrier sensing means it will sense the channel before transmission.
- Multiple access means if collision occur then it will wait for some time then retransmission occurs.

Working of a protocol

In **CSMA** Protocol if system want to send data it first senses the channel if channel is free then it will transmit otherwise it wait for some random time.

How it will sense?

- Generally, we represent 0 by +O voltage level and 1 by +5v
- If any unstandardized voltage level occur means, there is a collision in the channel.

Is this protocol being collision free?

- If two user sense the channel at the same time and that time channel is free then at this moment collision will occur. Therefore, this protocol is not a collision free protocol.
- There is no concept of **ack** here in CSMA protocol

Now how sender knows that this frame has been collide? In this protocol sender is not aware of collision because during transmission we does not sense the channel. To resolve this problem some Updation is done on CSMA protocol was done and new protocol came into existence i.e. CSMA/CD protocol. Here CD stands for Collision detection

Here in this protocol sender sense the channel during transmission also. In this protocol sender itself detect the collision, now how sender knows collision has been occurring. If sender transmitting the frame and at that time collision occur, then sender can detect collision.

Otherwise sender cannot detect collision. Now we will see how sender can detect collision

Diagram

- If t_x>=t_p + t_p then we can detect collision

  Length /R >= 2*D/S

  In CSMA/CD there is a restriction on minimum frame length.

- Now Efficiency of CSMA/CD protocol (Ethernet)

  μ=1/(1+5a)

  Here a= t_x / t_p

- This protocol is suitable for LAN not for MAN and WAN, as length increases efficiency decreases.

Diagram

Persistent CSMA/CD

- If system start sensing the channel, then it senses the channel until it does not gets channel free.

Non persistent CSMA/CD

- System will sense the channel before transmission if it does not get channel free, then it will wait for some time and then again start sensing the channel.

P-persistence

- If system got the channel free, then it has a probability p that it sends the data
- CSMA/CD is a theoretical protocol.

Practically implement protocol for delaying with collision (According to IEEE)

- 802.3(Ethernet)
- 802.4(Token Bus)
- 802.5(Token ring)

We will discuss Ethernet on the basic of four parameters.

- **Transmission protocol**
- **Signaling protocol**
- **Cableing protocol**
- **Frame protocol**

Ethernet

- **Transmission protocol**

  1 persistent CSMA/CD protocol

  If collision occur system wait for some random time then retransmit, this random time is decided by binary exponential back-off algorithm

  Binary exponential back-off algorithm says at ith collision system should choose a random number between 0 to 2^i -1

1st collision

- Random number is chosen in between 0 to 1

2nd collision

- Random number is chosen in between 0 to 3.
- If system choose a random number 0, then it will immediately send the data.

  If system, choose **random number 1** then system will start the channel after 1-bit slot

  1-bit slot=2 t_p

  Bit slot is a special word used in CSMA/CD protocol

- If we apply 15 times this algorithm, there is no problem after 15th collision i.e. at 15th collision and onwards data-link layer informs the higher layer that data was unable to deliver to receiver.

Question

After 4th collisions what is the probability that system will start immediately?

Solution:

0 to 2^4 -1

0 to 15

Total cases =16

Total number of favorable cases =1

Probability = favorable case/ total cases =1/16 →Answer

Question

A and B are only two station on an Ethernet LAN both A and B attempts to transmit and collide. What is the probability that A will win first back-off Algorithm?

Solution

A	B
0	0
1	1
0	1
1	0

A=0 and b=1 this is our favorable case

So p =1/4

Cs-2004 54 b

Signally standard

- Generally, we represent 0 by +0v and 1 by +5v but problem with this signally standard is that if we want to send bunch of 0's then we cannot distinguish between data and no data.
- For this two new encoding system was introduced

Differentially Manchester encoding scheme

Manchester encoding scheme

Manchester encoding scheme

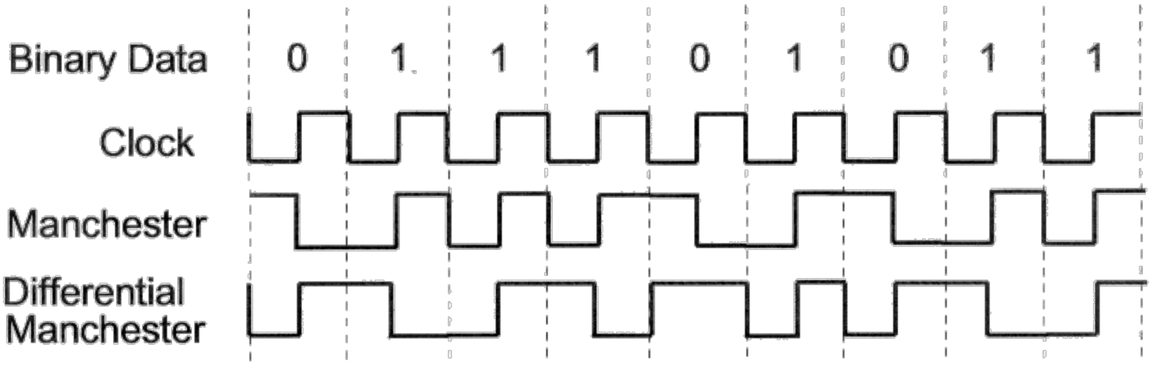
In Manchester encoding

1 is represent by Lower to Higher

0 is represent by Higher to Lower

Differential Manchester encoding

1 is represent by previous voltage- level and on the other hand 0 is represented by change in previous voltage-level.



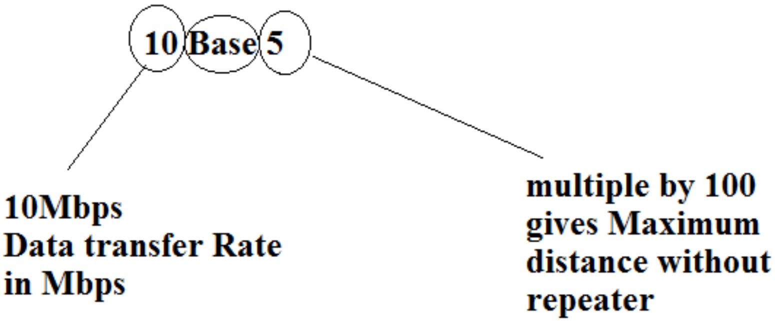
- Ethernet make use of differential Manchester encoding.

Baud rate

Change in voltage level per second is called baud rate on the other hand change in bits per second is called **bit rate**.

Baud rate =2-bit rate (in Manchester and differential Manchester encoding)

Caballing standard



10Mbps
Data transfer Rate
in Mbps

multiple by 100
gives Maximum
distance without
repeater

Frame format

Preamble	S D	Destination Address	Source Address	Optional	Length of Data	Data +Padding	CRC	ED
7 Byte	1 Byte	6 Byte	6 byte	2 Byte	2 Byte		4 Byte	1 Byte
							Trailer	

Preamble

- An Ethernet frame starts following a seven-byte preamble and one-byte start **frame delimiter** (SFD), both of which are part of the Ethernet packet enveloping the frame.
- The preamble of an Ethernet packet consists of a 56-bit (seven-byte) pattern of alternating 1 and 0 bits, allowing devices on the network to easily synchronize their receiver clocks, which is followed by the SFD to mark a new incoming frame.

SFD

- The SFD is the eight-bit (one-byte) value that marks the end of the preamble, which is the first field of an Ethernet packet, and indicates the beginning of the Ethernet frame. The SFD is designed to break the bit pattern of the preamble and signal the start of the actual frame

Destination and source address

- This field is of 6 bytes contain Mac address.

Type field

- It is an optional field. It shows whether that frame is data or control frame Since Ethernet is also based on 1-presistant CSMA/CD therefore there is a restriction on minimum frame size also
- In 802.3 LAN standard minimum frame length exclude preamble and including all necessary filed is 64 bytes. There is also restriction on minimum frame size it is 1500+ 26 , this 26 is of frame format
- Padding means if data is smaller than minimum size then we add some garbage. This garbage is knowns as padding.

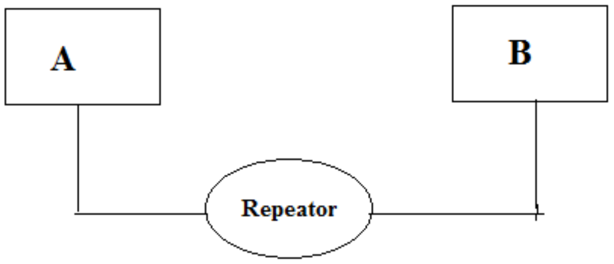
Drawback

- There is no concept of priority
- There is no guaranteed delivery of data
- To overcome drawback of **Ethernet** a new LAN-standard came into existence which is known as **Token-Ring**.

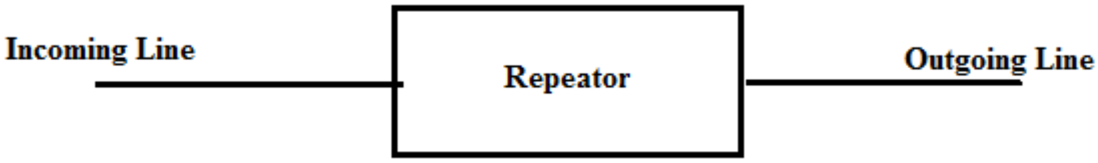
Different networking Device

Repeaters

- It is used to filer noise in the network. It works on physical layer.
- Repeaters connect different segment of LAN
- A repeater is a generator not an amplifier because amplifier does not distinguish between noise and signal it amplify both noise and signal but repeater extract the signal and removes all noise and regenerate signal

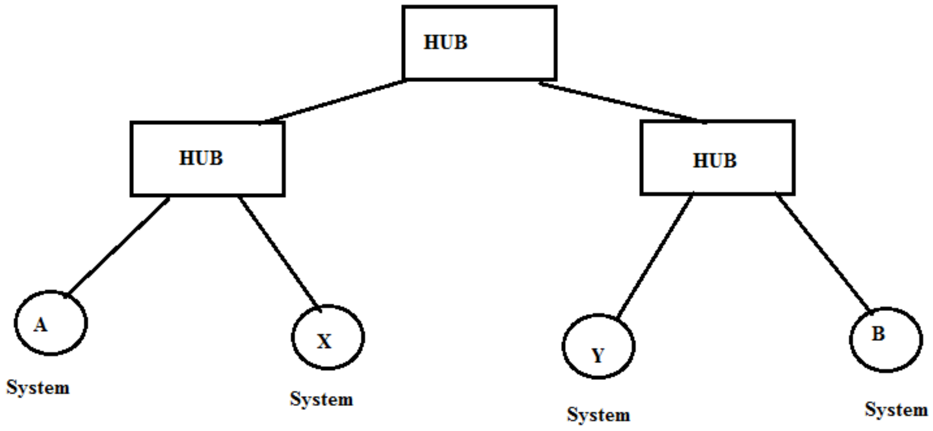


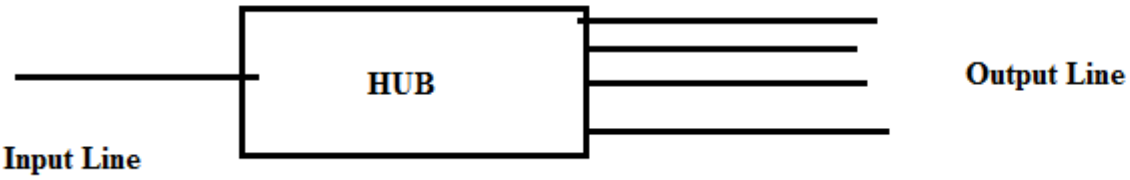
- Repeaters regenerate every frame it receives. In repeater one incoming file is there and one outgoing file is there.



Hub

Multiport repeaters are known as hub. hub can be used to create multilevel hierarchal of lan





- One input line and many output lines
- Hub is a broadcasting device.
- This device also works on physical layer.

Bridges

- Bridges can be used to connect two different Lan or the segment of very large LAN
- Bridges works on data-link-layer.
- This device is more intelligent then hub/repeaters but costly than hub/repeaters
- If it is HUB, then it will always broadcast but bridge filter the broadcast concept.

Diagram

On the basis of maintaining the mac addresses tale bridges are classified into three categories

- **Simple bridge**
- **Self-learning bridge**
- **Source routing bridge**

Simple bridge

- It is easy to implement.
- Entire table of bridge is maintaining manually. For maintaining table we have to implement program for that.

Drawback

- If we want to change the system in LAN, then we have to change manually in the table.

Self-learning bridges.

- Self-learning bridge maintain the mac address itself.
- By learning source address we design mac-address table.

Diagram

How bridges learn mac address.

Suppose I want to send data form A system which is in Lan1 to a system C which is present in lan3 then what will happen, first A will be broadcast the data frame in its lan as well as to the bridges the bridge will store the mac-address od A now what bridge has learnt it learnt that A is coming from lan1 if any system wants to send data to system A then bridge will forward that data to LAN1. In this way bridge will update its table.

Advantage

- If a change occurs on LAN, then it will automatically update to the table.

Disadvantage

- Problem of infinite loop

Diagram

Now I want to send frame from A to Z then what will happen? Firstly, B2 will broadcast then B1 will broadcast then B1 will broadcast. in this way infinite loop occur. To resolve this infinite loop problem spanning tree is used. Bridge together form the spanning tree of complete network. To create spanning tree, it is time consuming.

- Any change in network topology result in new spanning tree which are very time consuming

Source Routing Bridges

- In Source routing bridge, source will decide which route to be followed to send data to receiver. There is no maintenance of mac address table.
- Here there is a discovery frame which is used to decide which route to be followed.

For example

Diagram

Suppose I want to send data form system A to system C if B1 is **Source Routing Bridge** then first A will send discovery frame in which source address is there i.e. A then go to B1 in B1 bridge A lan1 B1 or A P1 B1 will be written then A P1 B1 C P2 B1. Now C will response to source of discovery frame. now A will send a frame with that path.

If network is too big then many discoveries frame will reach at destination but receiver response to first discovery frame that it received because that frame has chosen shorter route from sender to receiver.

Switches

- Form software point of view there is no difference between switches and bridge. But form hardware point of view there is a difference.
- Multiport bridges are knowns are **Switch.**
- Forwarding speed of frame is faster in switch as compare to bridges.
- There are two ways in which switches are forwarding their frame.

Stored and forward

Cut through

Store and forward

- In this mode, until we did not read whole frame we cannot forward it . After reading the whole frame switch/bridge take the decision.

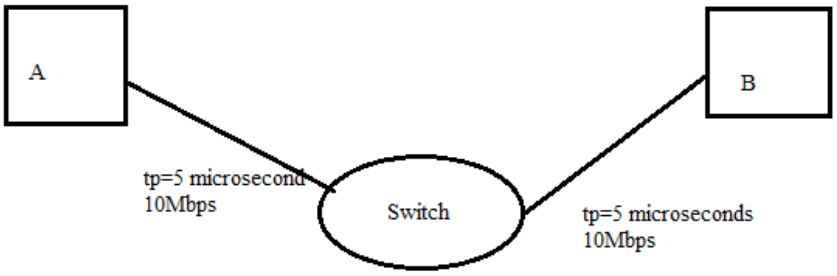
Cut through

- In this type of switch, after reading destination address they make forwarding decision. In this technique late checking is possible

Numerical based on different networking device

Consider the following problem

A system will send two frames to B System, each of 1000 bits. Find out how much time will be required to transverse second frame to system B (in microsecond)



Solution

T_x= length of data / bandwidth = 1000/ (10*10^6) =100micro second

Total time = $2*t_x + t_p + t_x + t_p$

=200+5+100+5=200+110=310 micro second