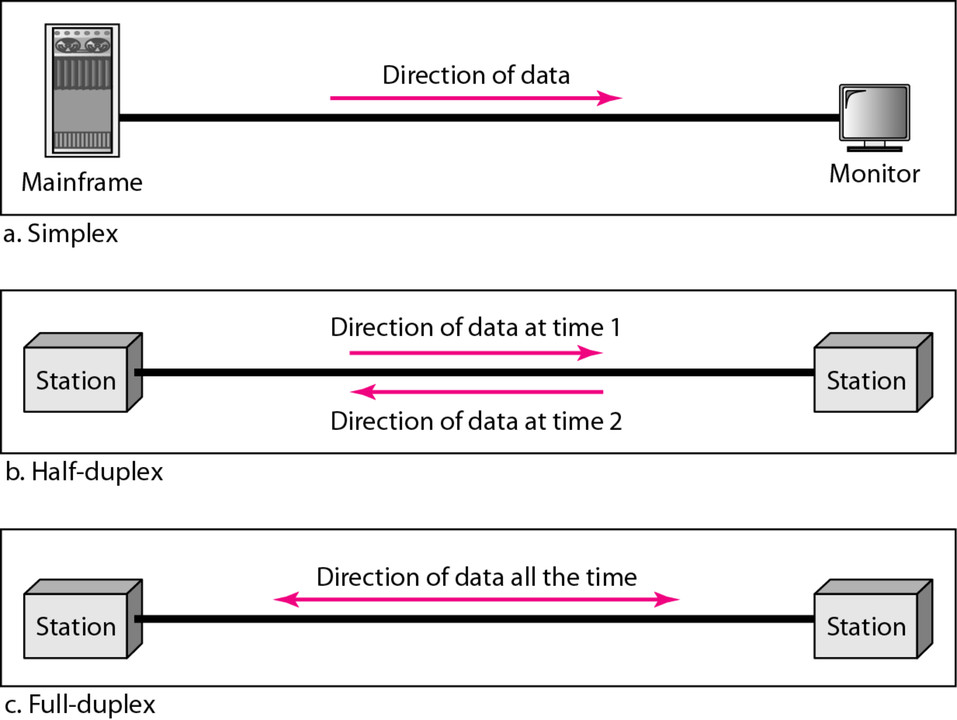
**1) Describe the types of communication between the devices with suitable diagram and examples (simplex, half duplex and full duplex)**

🡪



* Simplex
* Simplex is a communications mode in which only one signal is transmitted, and it always goes in the same direction .Simplex mode is a uni-directional communication. In simplex mode, Sender can send the data but that sender can’t receive the data. Simplex utilizes the maximum of a single bandwidth. Example of simplex mode are: Keyboard and monitor. The monitor cannot reply, or send any feedback, to the keyboard
* Half-duplex
* In half-duplex mode, Sender can send the data and also can receive the data one at a time. It is two-way directional communication but one at a time. Half Duplex mode is a two-way directional communication but one at a time In Half Duplex mode, Sender can send the data and also can receive the data but one at a time. It is suitable for those transmissions when there is requirement of sending data in both directions, but not at the same time. Example of half duplex mode is: Walkie-Talkies. the speakers at both ends can speak, but they have to speak one by one.  They cannot speak simultaneously.
* Full-duplex
* In full-duplex transmission mode, the communication between sender and receiver can occur simultaneously.  The sender and receiver can both transmit and receive at the same time. The full-duplex transmission mode is like a two-way road, in which traffic can flow in both directions at the same time. For example, in a telephone conversation, two people communicate, and both are free to speak and listen at the same time.

**2) List and explain the types of connection between the devices (Point-to-point and multipoint)**

🡪 There are two possible types of connections:

* point-to-point
* multipoint.

Point to point communication means the channel is shared between two devices. In this communication, There is dedicated link between two nodes.  
In this communication, the entire capacity is reserved between these connected two devices with the possibility of waste of network bandwidth resources .In this communication, there is one transmitter and one receiver .In point-to-point connections, the smallest distance is most important to reach the receiver.   
Point-to-point communication provides security and privacy because communication channel is not shared.

|  |
| --- |
| Multipoint Communication means the channel is shared among multiple devices or nodes. |
| In this communication, link is provided at all times for sharing the connection among nodes. |
| In this communication, there is one transmitter and many receivers. |
| In Multi-point connections, the smallest distance is not important to reach the receiver. |
| Multi-point communication does not provide security and privacy because communication channel is shared. |

**3) List and explain the physical topologies.**

🡪Network topologies describe the methods in which all the elements of a network are mapped. The topology term refers to both the physical and logical layout of a network.**Network Topology** is the physical layout of computers, cables, switches, routers, and other components of a network.

**4) What is hybrid topology, Explain with example?**

🡪It is the combination of two or more different topologies. For example, in a college we have so many departments, let us say one department uses ring topology and another department uses Star topology, connecting these two topologies which results in Hybrid Topology.

Hybrid= Ring+star

The features of Hybrid Topology are as follows −

* Hybrid Topology is the combination of two or more topologies.
* It inherits the advantages and disadvantages of other topologies also

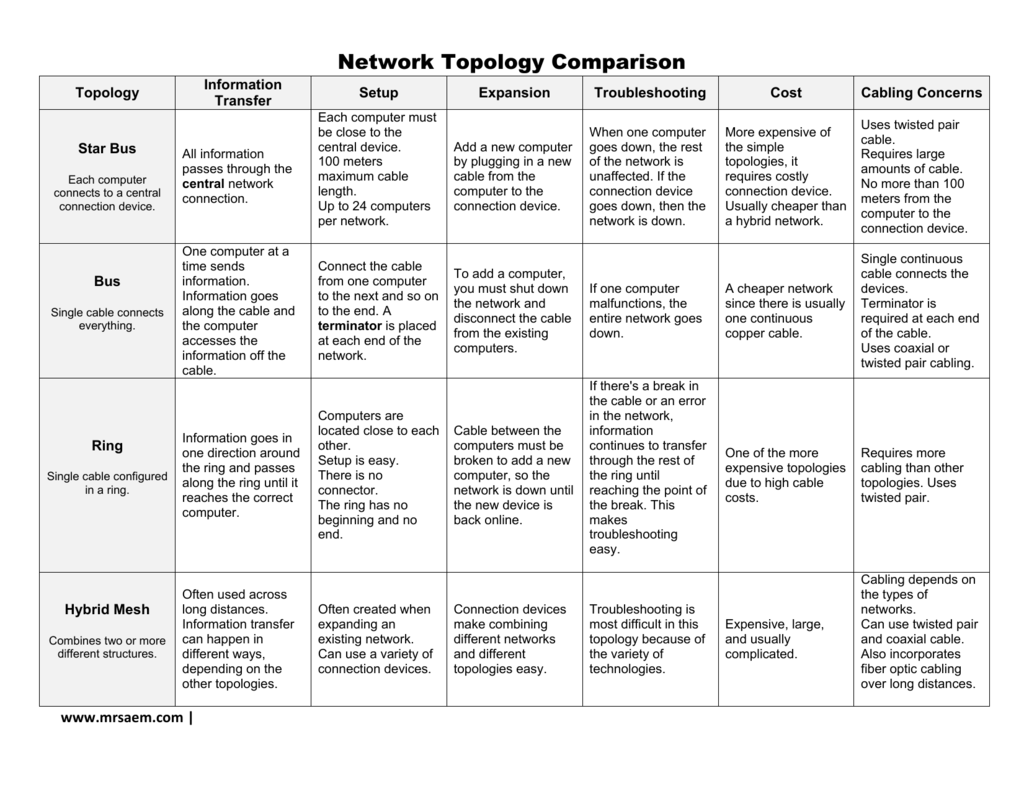
The advantages of Hybrid topology are given below −

* It is effective and flexible.
* Troubleshooting is easy.
* Error detecting is reliable.
* It is scalable because the size can be increased easily.

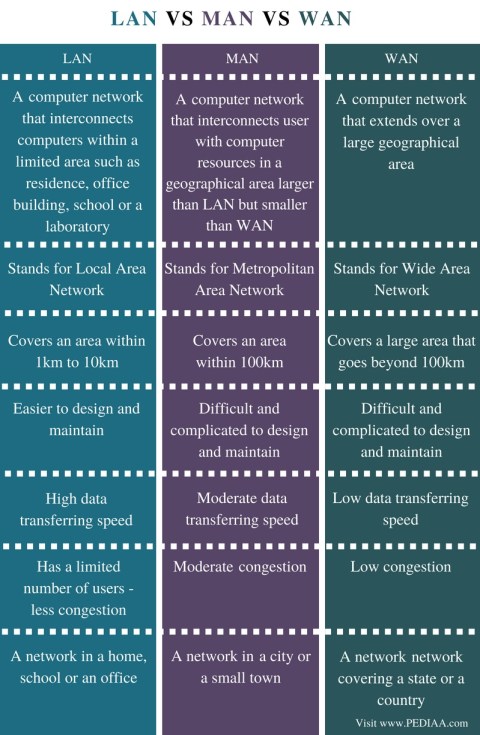
The disadvantages of Hybrid Topology are given below −

* Designing is difficult or complex.
* It is costly.

**5)Compare between topologies**

🡪

**6) Differentiate between LAN , MAN and WAN**



**7) Outline OSI Reference model and explain the each layer in detail.**

🡪

## In the OSI reference model, the communications between a computing system are split into seven different abstraction layers: Physical, Data Link, Network, Transport, Session, Presentation, and Application.

## Physical Layer

The lowest layer of the OSI Model is concerned with electrically or optically transmitting raw unstructured data bits across the network from the physical layer of the sending device to the physical layer of the receiving device. It can include specifications such as voltages, pin layout, cabling, and radio frequencies. At the physical layer, one might find “physical” resources such as network hubs, cabling, repeaters, network adapters or modems.

## Data Link Layer

At the data link layer, directly connected nodes are used to perform node-to-node data transfer where data is packaged into frames. The data link layer also corrects errors that may have occurred at the physical layer.

The data link layer encompasses two sub-layers of its own. The first, media access control (MAC), provides flow control and multiplexing for device transmissions over a network. The second, the logical link control (LLC), provides flow and error control over the physical medium as well as identifies line protocols.

## Network Layer

The network layer is responsible for receiving frames from the data link layer, and delivering them to their intended destinations among based on the addresses contained inside the frame. The network layer finds the destination by using logical addresses, such as IP (internet protocol). At this layer, routers are a crucial component used to quite literally route information where it needs to go between networks.

## Transport Layer

The transport layer manages the delivery and error checking of data packets. It regulates the size, sequencing, and ultimately the transfer of data between systems and hosts. One of the most common examples of the transport layer is TCP or the Transmission Control Protocol.

## Session Layer

The session layer controls the conversations between different computers. A session or connection between machines is set up, managed, and termined at layer 5. Session layer services also include authentication and reconnections.

## Presentation Layer

The presentation layer formats or translates data for the application layer based on the syntax or semantics that the application accepts. Because of this, it at times also called the syntax layer. This layer can also handle the encryption and decryption required by the application layer.

## Application Layer

At this layer, both the end user and the application layer interact directly with the software application. This layer sees network services provided to end-user applications such as a web browser or Office 365. The application layer identifies communication partners, resource availability, and synchronizes communication.

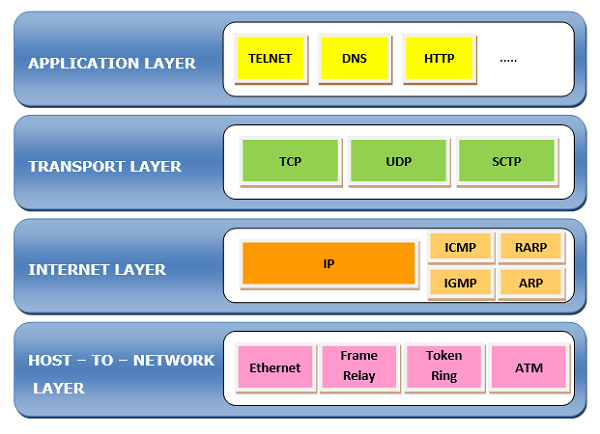
**8) Outline TCP/IP Reference model and explain the each layer in detail.**

CP/IP Reference Model is a four-layered suite of communication protocols. It was developed by the DoD (Department of Defence) in the 1960s. It is named after the two main protocols that are used in the model, namely, TCP and IP. TCP stands for Transmission Control Protocol and IP stands for Internet Protocol.

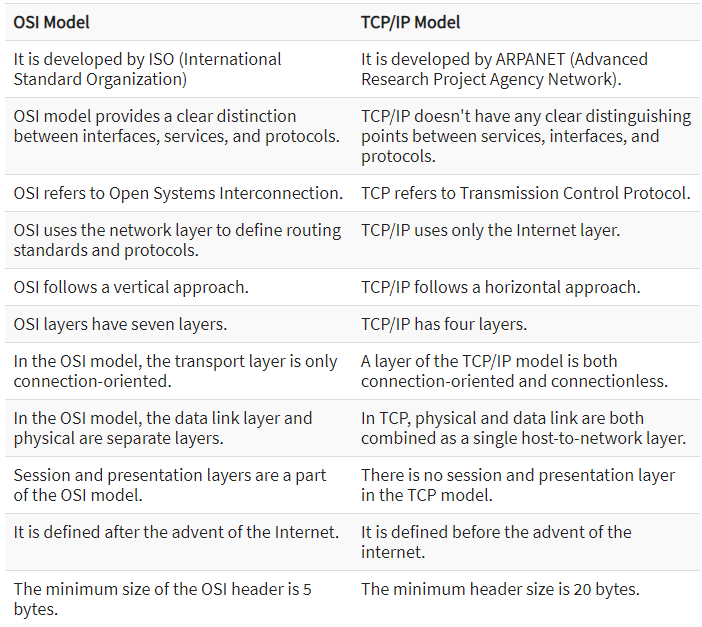
The four layers in the TCP/IP protocol suite are −

* **Host-to- Network Layer −**It is the lowest layer that is concerned with the physical transmission of data. TCP/IP does not specifically define any protocol here but supports all the standard protocols. This layer is mainly responsible for the transmission of the data between two devices on the same network. The functions carried out by this layer are encapsulating the IP datagram into frames transmitted by the network and mapping of IP addresses into physical addresses.
* **Internet Layer −**It defines the protocols for logical transmission of data over the network. The main protocol in this layer is Internet Protocol (IP) and it is supported by the protocols ICMP, IGMP, RARP, and ARP.
* ARP stands for **Address Resolution Protocol**.
* **ICMP** stands for Internet Control Message Protocol.
* ARP is a network layer protocol which is used to find the physical address from the IP address.
* **Transport Layer −** It is responsible for error-free end-to-end delivery of data. The protocols defined here are Transmission Control Protocol (TCP) and User Datagram Protocol (UDP).
* **Application Layer −** This is the topmost layer and defines the interface of host programs with the transport layer services. This layer includes all high-level protocols like Telnet, DNS, HTTP, FTP, SMTP, etc

The following diagram shows the layers and the protocols in each of the layers −



**9) Differentiate between OSI and TCP/IP reference model.**



**10) List the different networking devices &11) Note on following - Hub - Repeater - Bridge - Router - Switch - Gateway**

**🡪There are mainly 8 types of networking devices:**

* Hub
* Switch
* Router
* Bridge
* Gateway
* Modem
* Repeater
* Access Point

HUB

Hubs connect multiple computer networking devices together. A hub also acts as a repeater in that it amplifies signals that deteriorate after traveling long distances over connecting cables. A hub is the simplest in the family of network connecting devices because it connects LAN components with identical protocols.A hub can be used with both digital and analog data, provided its settings have been configured to prepare for the formatting of the incoming data. For example, if the incoming data is in digital format, the hub must pass it on as packets; however, if the incoming data is analog, then the hub passes it on in signal form.

Router

Routers help transmit packets to their destinations by charting a path through the sea of interconnected networking devices using different network topologies. Routers are intelligent devices, and they store information about the networks they’re connected to. are also used to translate from LAN framing to WAN framing. Router are also used to divide internal networks into two or more subnetworks. Routers are general-purpose devices that interconnect two or more heterogeneous networks. They are usually dedicated to special-purpose computers, with separate input and output network interfaces for each connected network

Repeater

A repeater is an electronic device that amplifies the signal it receives. You can think of repeater as a device which receives a signal and retransmits it at a higher level or higher power so that the signal can cover longer distances, more than 100 meters for standard LAN cables. Repeaters work on the Physical layer.

**Gateway**

Gateways normally work at the Transport and Session layers of the OSI model. At the Transport layer and above, there are numerous protocols and standards from different vendors; gateways are used to deal with them. Gateways provide translation between networking technologies such as Open System Interconnection (OSI) and Transmission Control Protocol/Internet Protocol (TCP/IP).  gateways connect two or more autonomous networks, each with its own routing algorithms, protocols, topology, domain name service, and network administration procedures and policies.

**Bridge**

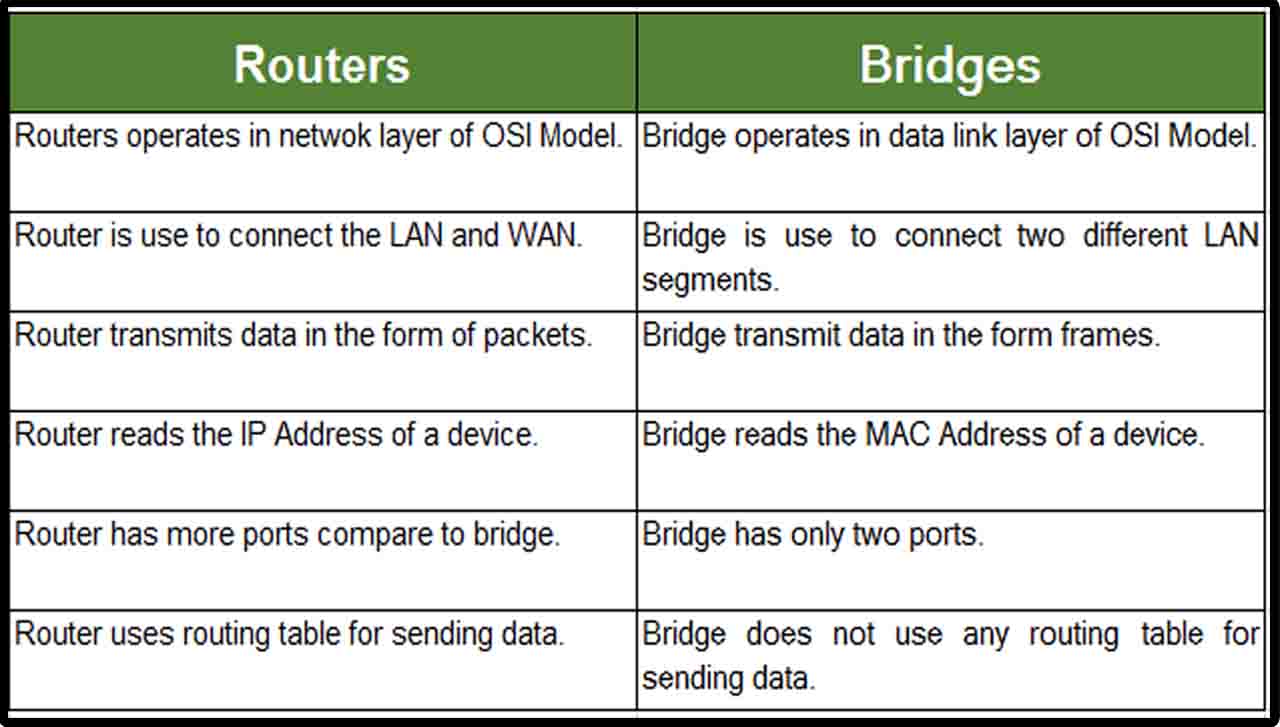
Bridges are used to connect two or more hosts or network segments together. The basic role of bridges in network architecture is storing and forwarding frames between the different segments that the bridge connects. They use hardware Media Access Control (MAC) addresses for transferring frames. By looking at the MAC address of the devices connected to each segment, bridges can forward the data or block it from crossing. Bridges can also be used to connect two physical LANs into a larger logical LAN.

**Switch**

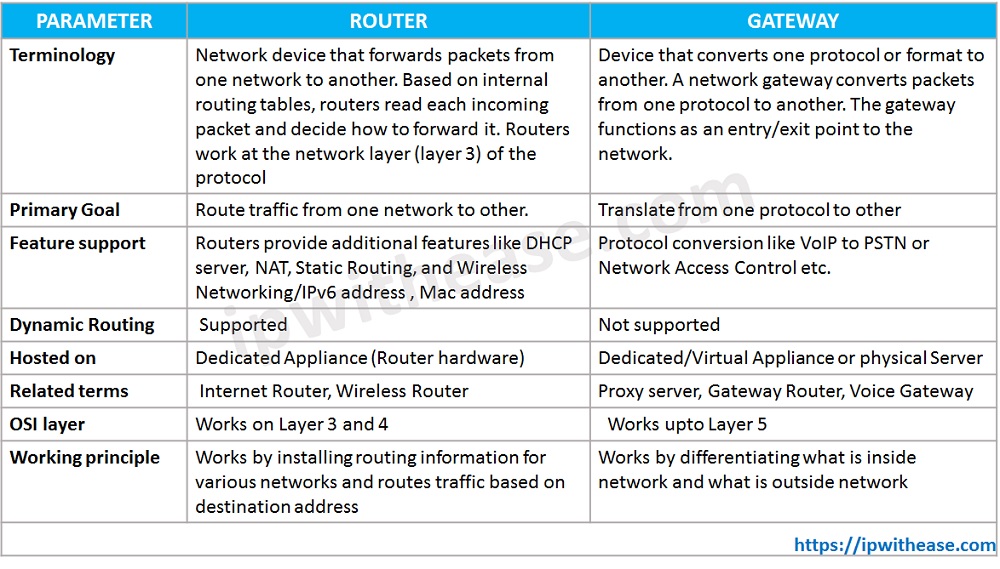
Switches generally have a more intelligent role than hubs. A switch is a multiport device that improves network efficiency. The switch maintains limited routing information about nodes in the internal network, and it allows connections to systems like hubs or routers. Strands of LANs are usually connected using switches. Generally, switches can read the hardware addresses of incoming packets to transmit them to the appropriate destination.

Using switches improves network efficiency over hubs or routers because of the virtual circuit capability. Switches also improve network security because the virtual circuits are more difficult to examine with network monitors

12)Compare Bridge and Router



**13)Compare Router and Gateway**



Q.1 List and explain the design Issues of the Data Link Layer.

🡪 [**Data-link layer**](https://www.geeksforgeeks.org/data-link-layer-in-osi-model/) is the second layer after the physical layer. The data link layer is responsible for maintaining the data link between two hosts or nodes. The data link layer is divided into two sub-layers :

[**Logical Link Control Sub-layer (LLC)**](https://practice.geeksforgeeks.org/problems/what-is-logical-link-control)**–**   
Provides the logic for the data link, Thus it controls the synchronization, flow control, and error checking functions of the data link layer.

1. **(i)** Error Recovery.
2. **(ii)** It performs the flow control operations.
3. **(iii)** User addressing.

[**Media Access Control Sub-layer (MAC)**](https://practice.geeksforgeeks.org/problems/what-is-media-access-controlmac)**–**   
It is the second sub-layer of data-link layer. It controls the flow and multiplexing for transmission medium. Transmission of data packets is controlled by this layer. Functions are –

* **(i)** To perform the control of access to media.
* **(ii)** It performs the unique addressing to stations directly connected to LAN.
* **(iii)** Detection of errors.

**Design issues with data link layer are :**

1. **Services provided to the network layer –**   
   The data link layer act as a service interface to the [network layer](https://www.geeksforgeeks.org/design-issues-in-network-layer/). The principle service is transferring data from network layer on sending machine to the network layer on destination machine. This transfer also takes place via DLL (Data link-layer).
2. [**Frame synchronization**](https://www.geeksforgeeks.org/framing-in-data-link-layer/)**–**   
   The source machine sends data in the form of blocks called frames to the destination machine. The starting and ending of each frame should be identified so that the frame can be recognized by the destination machine.
3. **Flow control –**   
   Flow control is done to prevent the flow of data frame at the receiver end. The source machine must not send data frames at a rate faster than the capacity of destination machine to accept them.
4. **Error control –**   
   Error control is done to prevent duplication of frames. The errors introduced during transmission from source to destination machines must be detected and corrected at the destination machine.

Q.2 List and Explain the services provided by Data Link Layer to Netwrok Layer

🡪 Data Link Layer is generally representing protocol layer in program that is simply used to handle and control the transmission of data between source and destination machines. It is simply responsible for exchange of frames among nodes or machines over physical network media. This layer is often closest and nearest to Physical Layer (Hardware).

#### **Unacknowledged Connectionless Service**

In this scenario, the source machine delivers data frames to the destination machine without expecting acknowledgement from them. The most common example of unacknowledged connectionless service is **Ethernet.**the sender and receiver do not establish any logical connection between them. Neither receiver provides any acknowledgement for the received frames. In case any frame is lost, the sender does not make any effort to detect or recover the lost frame.

#### **Acknowledged Connectionless Service**

As the name suggests, the sender and receiver do not establish any logical connection between them. But the receiver provides acknowledgement for the received frames. The most popular example of this kind of service is **WiFi.** If a frame is lost and the sender does not receive acknowledgement for the same within a specified time interval – the sender sends the frame again.

#### **Acknowledged Connection-Oriented Service**

With this kind of service, the sender and receiver initially establish a logical connection between them. Then each outgoing frame is sequentially numbered, guaranteeing that each frame will be delivered only once and in the right order. Once all the frames get delivered, the sender and receiver release the connection between them. The most popular example of this kind of service is **long distance telephone circuits.**

Q.3 What is framing ? What is need of framing. List the different framing Methods

🡪 A point-to-point connection called framing uses a wire to send data as a stream of bits between two computers or other devices. These pieces must be organised into comprehensible informational units. Data link layer functionality includes framing, and it offers a method for a sender to deliver a group of bits that are significant to the receiver. Each data link layer technology has its unique frame structure, including Ethernet, Frame Relay, Token Ring, and others. The headers of frames contain data like error-checking codes.

For example, a MAC address might be something like "00:11:22:33:44:55" or "00-11-22-33-44-55". MAC addresses are used by the data link layer to send and receive data over a network. They are used in conjunction with a protocol such as Ethernet to facilitate communication between devices on the same network.

Parts of a Frame

Here are the components of a frame:

* **Frame Header** − It includes the frame’s source and destination addresses.
* **Payload field** − It includes the message that needs to be spread.
* **Trailer** − The bits for error detection and repair are present.
* **Flag** − It designates the start and finish of the frame.

### **Fixed-sized Framing**

Since the frame’s size is constant in the fixed-sized framing, its length serves as its boundary. As a result, it is not necessary to use additional boundary bits to specify the beginning and end of the frame. ATM cells are an example of this.

### **Variable-sized Framing**

Each frame that needs to be transferred in this case may have a variable size. Therefore, additional processes are maintained to indicate when one frame ends and the next one begins. Local area networks employ it.

In variable-sized framing, there are two techniques to define frame delimiters:

* **Length Field** − Here, the size of the frame is decided by a length field. It is used in Ethernet (IEEE 802.3).
* **End Delimiter** − Here, the size of the frame is defined by a pattern that serves as a delimiter. In Token Rings, it is used. The following two methods are employed to prevent the problem if the pattern is present in the message.
  + **Byte Stuffing** − To distinguish the message from the delimiter, a byte is added. This technique is also known as character-oriented framing.
  + **Bit Stuffing** − To distinguish the message from the delimiter, a byte is added. This technique is also known as character-oriented framing.

Q.4 Explain Character Count with suitable example. Write the drawback of Character count method.

Data link layer translates the physical layers raw bit stream into discrete messages called frames. First framing method uses a field in the header to specify the number of characters in the frame. When the data link layer at the destination sees the character count, it knows how many characters follow and hence where the end of the frame is.

**For Example,**

Consider a data − 1 2 3 4 5 6 7 8 9 0 1 2 3

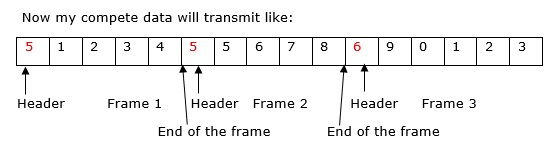
Divide this data into three frames −

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | 1 | 2 | 3 | 4 |

First empty box used for the header indicates character count.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | 5 | 6 | 7 | 8 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | 9 | 0 | 1 | 2 | 3 |



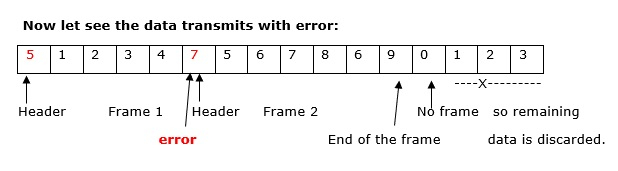
## Explanation

**Step 1** − Starting header in the frame indicate the character count, so first frame consists of 5 units of data including that number,

**Step 2** − Second frame header consists of 5 units of data including that number, so second frame consists of data 5,6,7,8. 8 indicate the end of the frame here.

**Step 3** − Third frame header consists of character count 6 that means the frame consists of 6 characters including 6. So the data in the third frame is 9,0,1,2,3.

**Step 4** − My data transfer to the receiver side without any errors.



## Explanation

**Step 1** − Starting header in the frame indicates the character count, so the first frame consists of 5 units of data including that number.

**Step 2** − Second frame header consists of 7 character count including that number actually it is an error, even though error is there the data will be transmitted, so second frame consists of data 5,6,7,8,6,9. Here, 9 indicate the end of the frame here.

**Step 3** − Third frame header consists of character count 0 that means the frame consists of 0 characters. The last frame data is discarded.

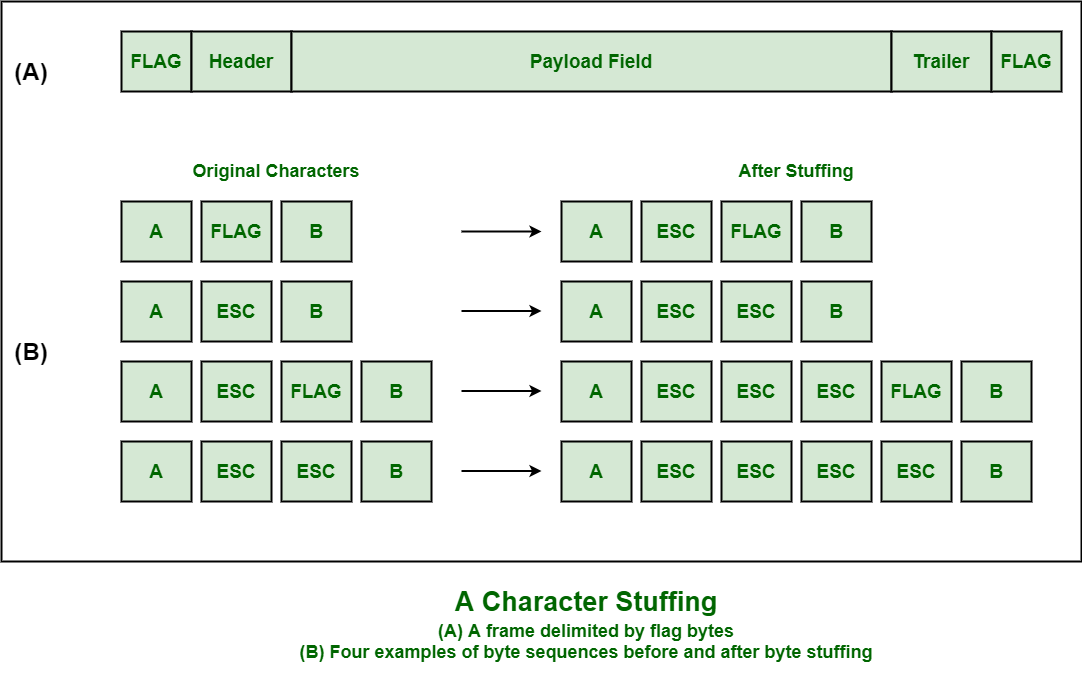
**Step 4** − My data transfer to the receiver side with errors.

The drawback is mainly, **if anyhow character count is disturbed or distorted by an error occurring during transmission, then destination or receiver might lose synchronization**.

Q. 5, Explain the character Stuffing with suitable example.

🡪 Character stuffing is also known as byte stuffing or character-oriented framing and is same as that of bit stuffing but byte stuffing actually operates on bytes whereas bit stuffing operates on bits. In byte stuffing, special byte that is basically known as ESC (Escape Character) that has predefined pattern is generally added to data section of the data stream or frame when there is message or character that has same pattern as that of flag byte.

But receiver removes this ESC and keeps data part that causes some problems or issues. In simple words, we can say that character stuffing is addition of 1 additional byte if there is presence of ESC or flag in text.



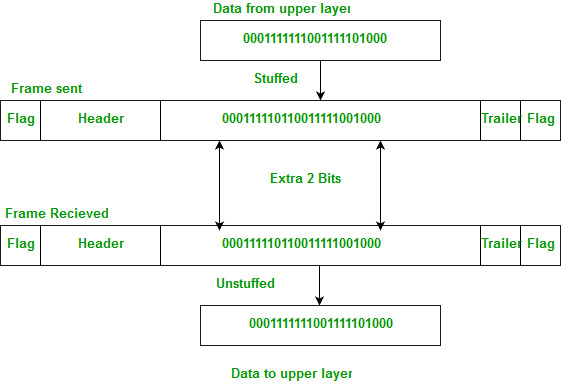
Q.6 Explain the bit Stuffing with suitable example.

🡪 Bit stuffing refers to the insertion of one or more [bits](https://www.techtarget.com/whatis/definition/bit-binary-digit) into a data transmission as a way to provide [signaling](https://www.techtarget.com/whatis/definition/signaling) information to a receiver. The receiver knows how to detect, remove or disregard the stuffed bits.

The data link layer is responsible for something called Framing, which is the division of stream of bits from network layer into manageable units (called frames). Frames could be of fixed size or variable size. In variable-size framing, we need a way to define the end of the frame and the beginning of the next frame.

**Bit stuffing** is the insertion of non information bits into data. Note that stuffed bits should not be confused with overhead bits.

**Overhead bits** are non-data bits that are necessary for transmission (usually as part of headers, checksums etc.).



**Applications of Bit Stuffing –**

1. synchronize several channels before multiplexing
2. rate-match two single channels to each other
3. run length limited coding

**Run length limited coding –** To limit the number of consecutive bits of the same value(i.e., binary value) in the data to be transmitted. A bit of the opposite value is inserted after the maximum allowed number of consecutive bits.

Bit stuffing technique does not ensure that the sent data is intact at the receiver side (i.e., not corrupted by transmission errors). It is merely a way to ensure that the transmission starts and ends at the correct places.

**Disadvantages of Bit Stuffing:**

* **The code rate is unpredictable; it depends on the data being transmitted.**
* **The stuffed bits do not contain any information.**

**Example of bit stuffing –**   
Bit sequence: 110101111101011111101011111110 (without bit stuffing)   
Bit sequence: 1101011111**0**01011111**0**101011111**0**110 (with bit stuffing)

After 5 consecutive 1-bits, a 0-bit is stuffed. Stuffed bits are marked bold.

Q.7 perform bit stuffing at sender side and de-stuffing at the receiver side for given data

🡪 // C program for the above approach

#include <stdio.h>

#include <string.h>

// Function for bit stuffing

void bitStuffing(int N, int arr[])

{

// Stores the stuffed array

int brr[30];

// Variables to traverse arrays

int i, j, k;

i = 0;

j = 0;

// Stores the count of consecutive ones

int count = 1;

// Loop to traverse in the range [0, N)

while (i < N) {

// If the current bit is a set bit

if (arr[i] == 1) {

// Insert into array brr[]

brr[j] = arr[i];

// Loop to check for

// next 5 bits

for (k = i + 1;

arr[k] == 1

&& k < N

&& count < 5;

k++) {

j++;

brr[j] = arr[k];

count++;

// If 5 consecutive set bits

// are found insert a 0 bit

if (count == 5) {

j++;

brr[j] = 0;

}

i = k;

}

}

// Otherwise insert arr[i] into

// the array brr[]

else {

brr[j] = arr[i];

}

i++;

j++;

}

// Print Answer

for (i = 0; i < j; i++)

printf("%d", brr[i]);

}

// Driver Code

int main()

{

int N = 6;

int arr[] = { 1, 1, 1, 1, 1, 1 };

bitStuffing(N, arr);

return 0;

}

Q.8 Draw the Binary Encoding, Manchester encoding, Differential Manchester encoding for given data.

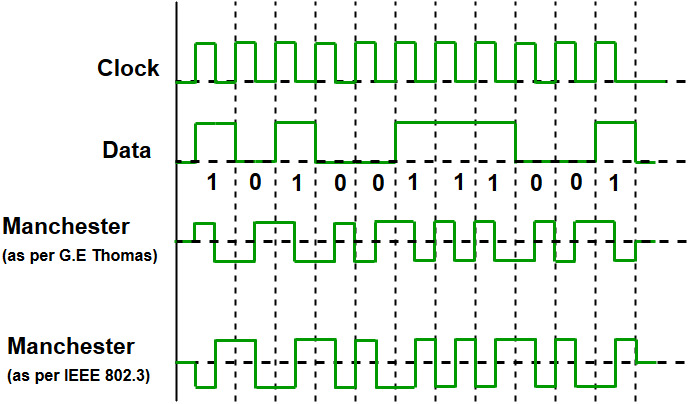
🡪

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 idea of RZ and the idea of-L are combined in Manchester.

In manchester duration of a bit is divided into two halves. The voltage remains the same at one level during the first half & moves to the other level.The transition at the middle of the bit provides synchronization.Differential Manchester,on the other hand,combines the idea of RZ and NRZ-I. There is always a transition at the middle of the bit, but the bit values are determined at the beginning of the bit. if next bit is zero there is transition if next bit is 1 there is none.

**Note:** Manchester encoding’s main advantage is signal synchronization.

# in this the value inside will change according to question



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 a lack of transmissions.   
It is of 2 types:

1. **NRZ-level encoding –**   
   The polarity of signals changes when the incoming signal changes from ‘1’ to ‘0’ or from ‘0’ to ‘1’. It considers the first bit of data as polarity change.
2. **NRZ-Inverted/ Differential encoding –**   
   In this, the transitions at the beginning of the bit interval are equal to 1 and if there is no transition at the beginning of the bit interval is equal to 0.

Q.9 Discuss the types of error with suitable example

🡪

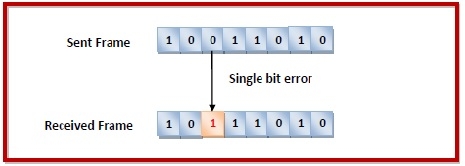
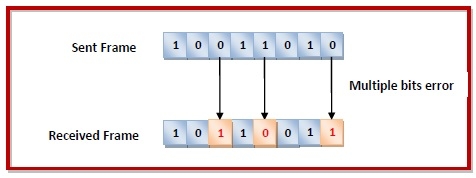
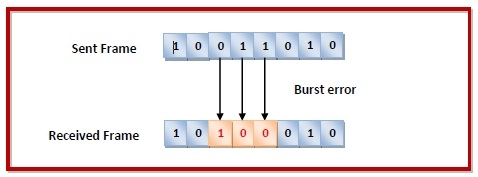
Data-link layer uses error control techniques to ensure that frames, i.e. bit streams of data, are transmitted from the source to the destination with a certain extent of accuracy.

## Errors

When bits are transmitted over the computer network, they are subject to get corrupted due to interference and network problems. The corrupted bits leads to spurious data being received by the destination and are called errors.

## Types of Errors

Errors can be of three types, namely single bit errors, multiple bit errors, and burst errors.

* **Single bit error** − In the received frame, only one bit has been corrupted, i.e. either changed from 0 to 1 or from 1 to 0.
* **Multiple bits error** − In the received frame, more than one bits are corrupted.
* **Burst error** − In the received frame, more than one consecutive bits are corrupted.

Q.10 List the different error detecting method

🡪

## There are three main techniques for detecting errors in frames: Parity Check, Checksum and Cyclic Redundancy Check (CRC). Parity Check

The parity check is done by adding an extra bit, called parity bit to the data to make a number of 1s either even in case of even parity or odd in case of odd parity.

While creating a frame, the sender counts the number of 1s in it and adds the parity bit in the following way

* In case of even parity: If a number of 1s is even then parity bit value is 0. If the number of 1s is odd then parity bit value is 1.
* In case of odd parity: If a number of 1s is odd then parity bit value is 0. If a number of 1s is even then parity bit value is 1.

On receiving a frame, the receiver counts the number of 1s in it. In case of even parity check, if the count of 1s is even, the frame is accepted, otherwise, it is rejected. A similar rule is adopted for odd parity check.

The parity check is suitable for single bit error detection only.

## Cyclic Redundancy Check (CRC)

Cyclic Redundancy Check (CRC) involves binary division of the data bits being sent by a predetermined divisor agreed upon by the communicating system. The divisor is generated using polynomials.

* Here, the sender performs binary division of the data segment by the divisor. It then appends the remainder called CRC bits to the end of the data segment. This makes the resulting data unit exactly divisible by the divisor.
* The receiver divides the incoming data unit by the divisor. If there is no remainder, the data unit is assumed to be correct and is accepted. Otherwise, it is understood that the data is corrupted and is therefore rejected.

## Checksum

In this error detection scheme, the following procedure is applied

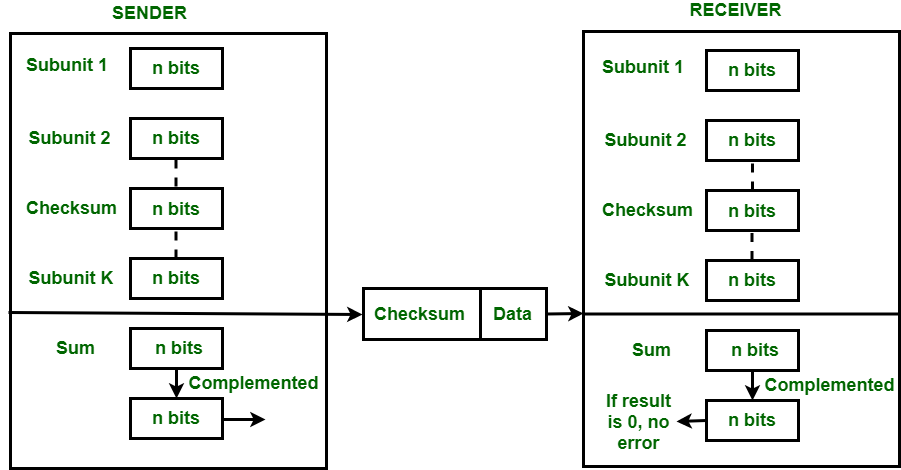
* Data is divided into fixed sized frames or segments.
* The sender adds the segments using 1’s complement arithmetic to get the sum. It then complements the sum to get the checksum and sends it along with the data frames.
* The receiver adds the incoming segments along with the checksum using 1’s complement arithmetic to get the sum and then complements it.
* If the result is zero, the received frames are accepted; otherwise, they are discarded.

Q.11 Explain how Checksum method is used for error detection, with Suitable example.

🡪

**Checksum** is the error detection method used by upper layer protocols and is considered to be more reliable than LRC, VRC and CRC. This method makes the use of **Checksum Generator** on Sender side and **Checksum Checker**on Receiver side.

At the Sender side, the data is divided into equal subunits of n bit length by the checksum generator. This bit is generally of 16-bit length. These subunits are then added together using one’s complement method. This sum is of n bits. The resultant bit is then complemented. This complemented sum which is called checksum is appended to the end of original data unit and is then transmitted to Receiver.



The Receiver after receiving data + checksum passes it to checksum checker. Checksum checker divides this data unit into various subunits of equal length and adds all these subunits. These subunits also contain checksum as one of the subunits. The resultant bit is then complemented. If the complemented result is zero, it means the data is error-free. If the result is non-zero it means the data contains an error and Receiver rejects it.

**Example –**  
If the data unit to be transmitted is 10101001 00111001, the following procedure is used at Sender site and Receiver site.

**Sender Site :**

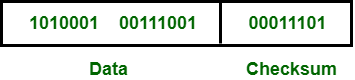
10101001 subunit 1

00111001 subunit 2

11100010 sum (using 1s complement)

**00011101**  checksum (complement of sum)

**Data transmitted to Receiver is –**



**Receiver Site :**

10101001 subunit 1

00111001 subunit 2

00011101 checksum

11111111 sum

**00000000** sum's complement

**Result is zero, it means no error.**

**Advantage :**   
The checksum detects all the errors involving an odd number of bits as well as the error involving an even number of bits.

**Disadvantage :**   
The main problem is that the error goes undetected if one or more bits of a subunit is damaged and the corresponding bit or bits of a subunit are damaged and the corresponding bit or bits of opposite value in second subunit are also damaged. This is because the sum of those columns remains unchanged.

**Example –**   
If the data transmitted along with checksum is 10101001 00111001 00011101. But the data received at destination is **0**0101001 **1**0111001 00011101.

**Receiver Site :**

**0**0101001 1st bit of subunit 1 is damaged

**1**0111001 1st bit of subunit 2 is damaged

00011101 checksum

11111111 sum

00000000 Ok 1's complement

Although data is corrupted, the error is undetected.

Q.12 Find hamming code for 4 bit data “ 1101”

Hamming (7, 4) code: It is a linear error-correcting code that encodes four bits of data into seven bits, by adding three parity bits. Example: It is used in the Bell-Telephone laboratory, error-prone punch caret reader to detect the error and correct them.

Hamming code:

Bits # 1 2 3 4 5 6 7

Transmitted bits P1 P2 d1 P3 d2 d3 d4

  P1 = d1 ⊕ d2 ⊕ d4

P2 = d1 ⊕ d4 ⊕ d3

P3 = d2 ⊕ d4 ⊕ d3

Solution: Given data 1101 i.e.

d1 = 1, d2 = 1, d3 = 0, d4 = 1

We can write:

P1 = d1 ⊕ d2 ⊕ d4 = 1 ⊕ 1 ⊕ 1 = 1

P2 = d1 ⊕ d4 ⊕ d3 = 1 ⊕ 1 ⊕ 0 = 0

P3 = d2 ⊕ d4 ⊕ d3 = 1 ⊕ 1 ⊕ 0 = 0

Then transmitted final code is

P1 P2 d1 P3 d2 d3 d4

1 0 1 0 1 0 1

i.e. 1010101

Q.13 What is sliding window (sender and receiver sliding window)

🡪 Sliding window protocols are data link layer protocols for reliable and sequential delivery of data frames. The sliding window is also used in Transmission Control Protocol.

In this protocol, multiple frames can be sent by a sender at a time before receiving an acknowledgment from the receiver. The term sliding window refers to the imaginary boxes to hold frames. Sliding window method is also known as windowing.

## Working Principle

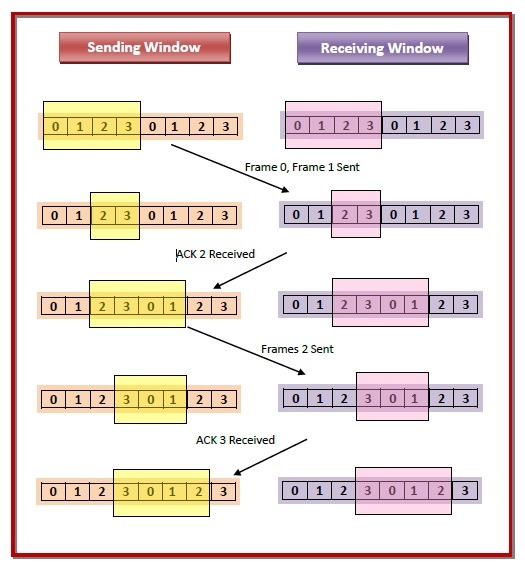
In these protocols, the sender has a buffer called the sending window and the receiver has buffer called the receiving window.

The size of the sending window determines the sequence number of the outbound frames. If the sequence number of the frames is an n-bit field, then the range of sequence numbers that can be assigned is 0 to 2𝑛−1. Consequently, the size of the sending window is 2𝑛−1. Thus in order to accommodate a sending window size of 2𝑛−1, a n-bit sequence number is chosen.

The sequence numbers are numbered as modulo-n. For example, if the sending window size is 4, then the sequence numbers will be 0, 1, 2, 3, 0, 1, 2, 3, 0, 1, and so on. The number of bits in the sequence number is 2 to generate the binary sequence 00, 01, 10, 11.

The size of the receiving window is the maximum number of frames that the receiver can accept at a time. It determines the maximum number of frames that the sender can send before receiving acknowledgment.

## Example

Suppose that we have sender window and receiver window each of size 4. So the sequence numbering of both the windows will be 0,1,2,3,0,1,2 and so on. The following diagram shows the positions of the windows after sending the frames and receiving acknowledgments. 

## Types of Sliding Window Protocols

The Sliding Window ARQ (Automatic Repeat reQuest) protocols are of two categories −



* **Go – Back – N ARQ**

Go – Back – N ARQ provides for sending multiple frames before receiving the acknowledgment for the first frame. It uses the concept of sliding window, and so is also called sliding window protocol. The frames are sequentially numbered and a finite number of frames are sent. If the acknowledgment of a frame is not received within the time period, all frames starting from that frame are retransmitted.

* **Selective Repeat ARQ**

This protocol also provides for sending multiple frames before receiving the acknowledgment for the first frame. However, here only the erroneous or lost frames are retransmitted, while the good frames are received and buffered.

1.Explain the Dynamic Channel Allocation and List the different Multiple Access Protocols

🡪

A group of protocols known as multiple access protocols work within the Open Systems Interconnection (OSI) model’s Medium Access Control (MAC) sublayer. Multiple nodes or users can access a shared network channel due to these technologies.

Data transmission between two nodes is handled by the Data Link Layer. Its primary duties include data link control and multiple access control

## 1. Random Access Protocol

All stations in the random access protocol have equal superiority, which means that no station has higher priority than any other station. Depending on the status of the medium, any station may send data ( idle or busy). It has two attributes:

* There is no set timing for data transmission.
* The order of the stations delivering data is not fixed.

The following are divisions of the random access protocols:

### **(a) ALOHA**

Although ALOHA was created for wireless LAN, it can also be used for shared mediums. This allows for simultaneous data transmission from numerous stations, which might cause collisions and jumbled data.

### **(b) CSMA**

Fewer collisions are guaranteed by carrier sensing multiple access (CSMA) since the station must first determine whether the medium is busy or idle before delivering data. If it isn’t idle, it waits for the channel to become idle before sending data. Due to propagation latency, there is still a potential for collision in CSMA.

### **(c) CSMA/CD**

CSMA/CD is an abbreviation of Carrier Sense Multiple Access/Collision Detection. It refers to the multiple access carrier with collision detection. In CSMA/CD, all the stations have the ability to stop data transmission if a collision is found anywhere.

### **(d) CSMA/CA**

CSMA/CA is an abbreviation of Carrier Sense Multiple Access/Collision Avoidance. Multiple access with carrier awareness and collision avoidance, sender receipt of acknowledgement signals is a necessary step in the collision detection process.

 Controlled Access Protocol

In this, the station sends the data once it has received approval from all other stations. The stations under controlled access exchange information to determine which station has the authority to send. In order to prevent message collisions over a shared medium, it only permits one node to send at a time. These are the three controlled-access techniques:

* Token Passing
* Polling
* Reservation

## 3. Channelization

The channelization protocol allows numerous stations to access the same channel at the same time by sharing the link’s available bandwidth according to time, frequency, and code. The three types of channelization are: Frequency Division Multiple Access, Time Division Multiple Access and Code Division Multiple Access.

1. What is random access protocol? List the random-access protocol

nnelization.

## 1. Random Access Protocol

All stations in the random access protocol have equal superiority, which means that no station has higher priority than any other station. Depending on the status of the medium, any station may send data ( idle or busy). It has two attributes:

* There is no set timing for data transmission.
* The order of the stations delivering data is not fixed.

The following are divisions of the random access protocols:

### **(a) ALOHA**

Although ALOHA was created for wireless LAN, it can also be used for shared mediums. This allows for simultaneous data transmission from numerous stations, which might cause collisions and jumbled data.

### **(b) CSMA**

Fewer collisions are guaranteed by carrier sensing multiple access (CSMA) since the station must first determine whether the medium is busy or idle before delivering data. If it isn’t idle, it waits for the channel to become idle before sending data. Due to propagation latency, there is still a potential for collision in CSMA.

For instance, station A will sense the medium before sending any data. It will begin sending data if it discovers that the channel is empty. However, if station B wishes to send data and senses the medium, it will also find it idle and send data at the same time the first bits of information are transferred from station A (delayed owing to propagation delay). As a result, data from stations A and B will collide.

Here are the CSMA access modes:

* **Non-persistent:** The node senses the channel; if it is free, it sends the data; if not, it checks the medium once or twice (not continuously) and sends the data when it is.
* **1-persistent:**The node senses the channel, sends the data if it is idle, or constantly checks the medium for idleness before sending data unconditionally (with a probability of 1) when the channel becomes idle.
* **P-persistent:**The node senses the media and sends data with p probability if it is idle. If the data is not transferred ((1-p) probability), the system waits a while before checking the media once more. If the medium is still empty, the system sends the data with a p probability. This process will repeat until the frame is sent. It is used in packet radio and Wifi systems.
* **O-persistent:** Transmission takes place in the sequence determined by the superiority of nodes. The node waits because of its time slot in order to send data if the medium is not in use.

### **(c) CSMA/CD**

CSMA/CD is an abbreviation of Carrier Sense Multiple Access/Collision Detection. It refers to the multiple access carrier with collision detection. In CSMA/CD, all the stations have the ability to stop data transmission if a collision is found anywhere.

### **(d) CSMA/CA**

CSMA/CA is an abbreviation of Carrier Sense Multiple Access/Collision Avoidance. Multiple access with carrier awareness and collision avoidance, sender receipt of acknowledgement signals is a necessary step in the collision detection process. The data is successfully delivered if there is just one signal (its own), but a collision has occurred if there are two signals (its own and that with which it collided). The collision must significantly affect the received signal in order to discriminate between these two scenarios. However, this is not the case in wired networks, which is why CSMA/CA is employed here.

The CSMA/CA prevents collisions by:

1. **Interframe space**– In order to prevent collisions caused by propagation delays, the station waits for the medium to become idle before sending data. This waiting period is known as the Interframe Space (IFS). Once more, it checks to see if the medium is idle after this. The priority of the station affects the IFS duration.
2. **Contention Window**– The quantity of time has been broken up into slots. When the transmitter is prepared to send data, the number of wait slots it chooses at random doubles each time the medium is not discovered to be idle. If the medium is determined to be in use, the process is not restarted in its entirety; rather, the timer is restarted when the channel is once more found to be inactive.
3. **Acknowledgement**– If the acknowledgement is just not received before time-out, the sender resends the data.

Explain CSMA along with 1 - persistent CSMA , Non persistent CSMA and P – persistent CSMA

🡪

It is a **carrier sense multiple access** based on media access protocol to sense the traffic on a channel (idle or busy) before transmitting the data. It means that if the channel is idle, the station can send data to the channel. Otherwise, it must wait until the channel becomes idle. Hence, it reduces the chances of a collision on a transmission medium.

1 - persistent CSMA

in 1-persistent CSMA, the station continuously senses the channel to check its state i.e. idle or busy so that it can transfer data or not. In case when the channel is busy, the station will wait for the channel to become idle. When station found idle channel, it transmits the frame to the channel without any delay. It transmits the frame with probability 1. Due to probability 1, it is called 1-persistent CSMA. The problem with this method is that there are a large number of chances for the collision it is because there is a chance when two or more stations found channel in idle state and the transmit frames at the same time. On the time when collision occurs the station has to wait for the random time for the channel to be idle and to start all again.

P – persistent CSMA

P-persistent CSMA is an approach of Carrier Sense Multiple Access (CMSA) protocol that combines the advantages of 1-persistent CMSA and non-persistent CMSA. Using CMSA protocols, more than one users or nodes send and receive data through a shared medium that may be a single cable or optical fiber connecting multiple nodes, or a portion of the wireless spectrum.

In p-persistent CSMA, when a transmitting station has a frame to send and it senses a busy channel, it waits for the end of the transmission, and then transmits with a probability p. Since, it sends with a probability p, the name p – persistent CSMA is given.

## Algorithm

The algorithm of p-persistent CMSA is:

* When a frame is ready, the transmitting station checks whether the channel is idle or busy.
* If the channel is idle then it transmits the frame immediately.
* If the channel is busy, the station waits and continually checks until the channel becomes idle.
* When the channel becomes idle, the station transmits the frame with a probability p.
* With a probability ( 1 – p ), the channel waits for next time slot. If the next time slot is idle, it again transmits with a probability p and waits with a probability ( 1 – p ).
* The station repeats this process until either frame has been transmitted or another station has begun transmitting.
* If another station begins transmitting, the station waits for a random amount of time and restarts the algorithm.

## Advantage of p-persistent CSMA

It is the most efficient among 1-persistent CSMA, non-persistent CSMA and p-persistent CSMA. It reduces the number of collisions considerably as compared to 1-persistent CSMA. The channel utilization is much better than non-persistent CSMA.

Non persistent CSMA

Non-persistent CSMA is a non – aggressive version of Carrier Sense Multiple Access (CMSA) protocol that operates in the Medium Access Control (MAC) layer. Using CMSA protocols, more than one users or nodes send and receive data through a shared medium that may be a single cable or optical fiber connecting multiple nodes, or a portion of the wireless spectrum.

In non-persistent CSMA, when a transmitting station has a frame to send and it senses a busy channel, it waits for a random period of time without sensing the channel in the interim, and repeats the algorithm again.

## Algorithm

The algorithm of non-persistent CMSA is

* When a frame is ready, the transmitting station checks whether the channel is idle or busy.
* If the channel is idle then it transmits the frame immediately.
* If the channel is busy, the station waits for a random time period during which it does not check whether the channel is idle or busy.
* At the end of the waiting time period, it again checks the status of the channel and restarts the algorithm.

## Advantage of non-persistent CSMA

It rate of collisions is much reduced than 1-persistent CMSA. This is because each station waits for a random amount of time before attempting retransmission.

## Disadvantage of non-persistent CSMA

It reduces the bandwidth usage of network. This is because the channel remains idle even if there are stations who have frames to transmit. This occurs since each station wait for a random time before attempting retransmission. There may be multiple stations who are waiting while the channel is idle.

Explain the CSMA with Collision Detection (CSMA/CD) along with algorithm

Carrier Sense Multiple Access with Collision Detection (CSMA/CD) is a network protocol for carrier transmission that operates in the Medium Access Control (MAC) layer. It senses or listens whether the shared channel for transmission is busy or not, and defers transmissions until the channel is free. The collision detection technology detects collisions by sensing transmissions from other stations. On detection of a collision, the station stops transmitting, sends a jam signal, and then waits for a random time interval before retransmission.

## Algorithms

The algorithm of CSMA/CD is:

* When a frame is ready, the transmitting station checks whether the channel is idle or busy.
* If the channel is busy, the station waits until the channel becomes idle.
* If the channel is idle, the station starts transmitting and continually monitors the channel to detect collision.
* If a collision is detected, the station starts the collision resolution algorithm.
* The station resets the retransmission counters and completes frame transmission.

The algorithm of Collision Resolution is:

* The station continues transmission of the current frame for a specified time along with a jam signal, to ensure that all the other stations detect collision.
* The station increments the retransmission counter.
* If the maximum number of retransmission attempts is reached, then the station aborts transmission.
* Otherwise, the station waits for a backoff period which is generally a function of the number of collisions and restart main algorithm.
* Though this algorithm detects collisions, it does not reduce the number of collisions.
* It is not appropriate for large networks performance degrades exponentially when more stations are added.

7. What is Binary exponential Back-off Algorith

Back-off algorithm is a **collision resolution** mechanism which is used in random access MAC protocols (CSMA/CD). This algorithm is generally used in Ethernet to schedule re-transmissions after collisions.

If a collision takes place between 2 stations, they may restart transmission as soon as they can after the collision. This will always lead to another collision and form an infinite loop of collisions leading to a deadlock. To prevent such scenario back-off algorithm is used.

Let us consider an scenario of 2 stations A and B transmitting some data:



After a collision, time is divided into discrete slots (**Tslot**) whose length is equal to 2t, where t is the maximum propagation delay in the network.

The stations involved in the collision randomly pick an integer from the set K i.e {0, 1}. This set is called the contention window. If the sources collide again because they picked the same integer, the contention window size is doubled and it becomes {0, 1, 2, 3}. Now the sources involved in the second collision randomly pick an integer from the set {0, 1, 2, 3} and wait for that number of time slots before trying again. Before they try to transmit, they listen to the channel and transmit only if the channel is idle. This causes the source which picked the smallest integer in the contention window to succeed in transmitting its frame.

So, Back-off algorithm defines a *waiting time for the stations involved in collision*, i.e. for how much time the station should wait to re-transmit.

Waiting time = back–off time

Waiting time = K \* Tslot

where K = [0, 2n – 1 ]

Describe the CSMA/CA

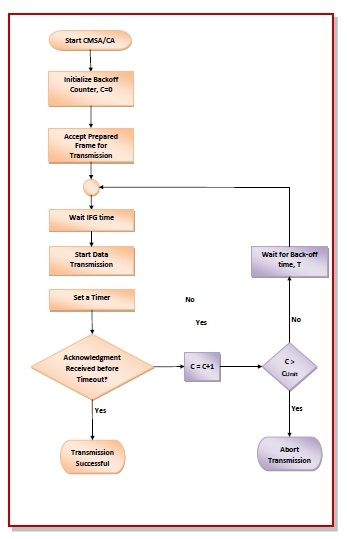
Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) is a network protocol for carrier transmission that operates in the Medium Access Control (MAC) layer. In contrast to CSMA/CD (Carrier Sense Multiple Access/Collision Detection) that deals with collisions after their occurrence, CSMA/CA prevents collisions prior to their occurrence.

## Algorithm

The algorithm of CSMA/CA is:

* When a frame is ready, the transmitting station checks whether the channel is idle or busy.
* If the channel is busy, the station waits until the channel becomes idle.
* If the channel is idle, the station waits for an Inter-frame gap (IFG) amount of time and then sends the frame.
* After sending the frame, it sets a timer.
* The station then waits for acknowledgement from the receiver. If it receives the acknowledgement before expiry of timer, it marks a successful transmission.
* Otherwise, it waits for a back-off time period and restarts the algorithm.

The following flowchart summarizes the algorithms:



## Advantages of CMSA/CD

* CMSA/CA prevents collision.
* Due to acknowledgements, data is not lost unnecessarily.
* It avoids wasteful transmission.
* It is very much suited for wireless transmissions.

## Disadvantages of CSMA/CD

* The algorithm calls for long waiting times.
* It has high power consumption.

9. What is CONTROLLED ACCESS/ Collision free Protocol and list the Collision free Protocols

Almost collisions can be avoided in **CSMA/CD**.they can still occur during the contention period.the collision during contention period adversely affects the system performance, this happens when the cable is long and length of packet are short. This problem becomes serious as fiber optics network come into use. Here we shall discuss some protocols that resolve the collision during the contention period.

* Bit-map Protocol
* Binary Countdown
* Limited Contention Protocols
* The Adaptive Tree Walk Protocol

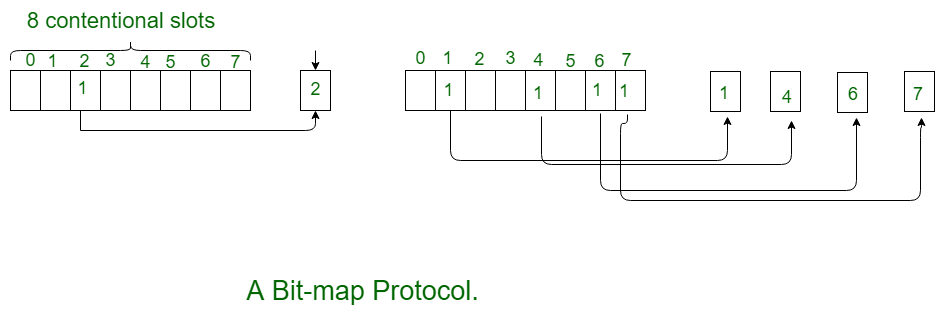
Pure and slotted Aloha, CSMA and CSMA/CD are **Contention based Protocols:**

* Try-if collide-Retry
  + No guarantee of performance
    - What happen if the network load is high?

**Collision Free Protocols:**

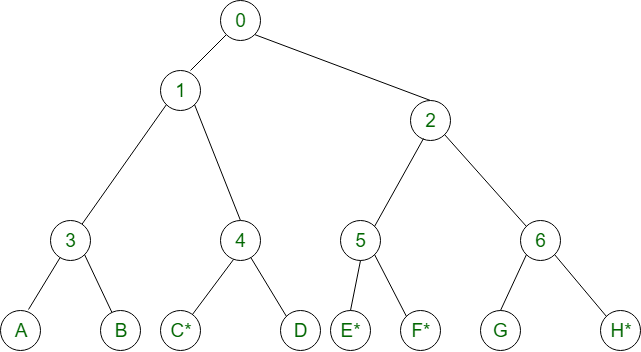
* + - Pay constant overhead to achieve performance guarantee
    - Good when network load is high

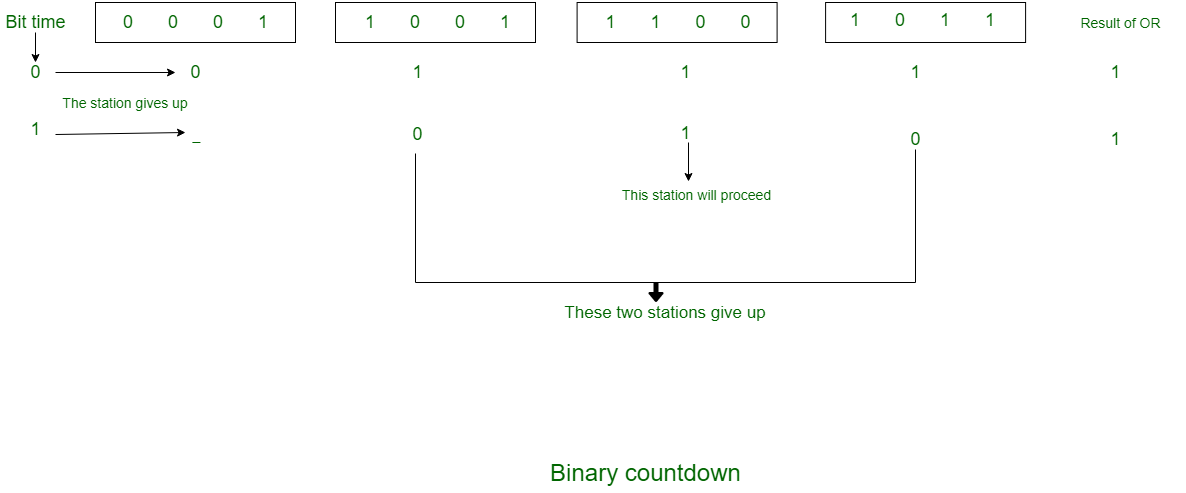
**1. Bit-map Protocol:**  
Bit map protocol is collision free Protocol in In bitmap protocol method, each contention period consists of exactly N slots. if any station has to send frame, then it transmits a 1 bit in the respective slot. For example if station 2 has a frame to send, it transmits a 1 bit during the second slot.

In general Station 1 Announce the fact that it has a frame questions by inserting a 1 bit into slot 1. In this way, each station has complete knowledge of which station wishes to transmit. There will never be any collisions because everyone agrees on who goes next. Protocols like this in which the desire to transmit is broadcasting for the actual transmission are called *Reservation Protocols*.  
  
  
  
  
  
For analyzing the performance of this protocol, We will measure time in units of the contention bits slot, with a data frame consisting of *d* time units. Under low load conditions, the bitmap will simply be repeated over and over, for lack of data frames.All the stations have something to send all the time at high load, the N bit contention period is prorated over N frames, yielding an overhead of only 1 bit per frame.

Generally, high numbered stations have to wait for half a scan before starting to transmit low numbered stations have to wait for half a scan(N/2 bit slots) before starting to transmit, low numbered stations have to wait on an average 1.5 N slots.  
  
  
**2. Binary Countdown:**  
Binary countdown protocol is used to overcome the overhead 1 bit per binary station. In binary countdown, binary station addresses are used. A station wanting to use the channel broadcast its address as binary bit string starting with the high order bit. All addresses are assumed of the same length. Here, we will see the example to illustrate the working of the binary countdown.

In this method, different station addresses are ORed together who decide the priority of transmitting. If these stations 0001, 1001, 1100, 1011 all are trying to seize the channel for transmission. All the station at first broadcast their most significant address bit that is 0, 1, 1, 1 respectively. The most significant bits are ORed together. Station 0001 see the 1MSB in another station addresses and knows that a higher numbered station is competing for the channel, so it gives up for the current round.

Other three stations 1001, 1100, 1011 continue. The next bit is 1 at station 1100, swiss station 1011 and 1001 give up. Then station 110 starts transmitting a frame, after which another bidding cycle starts.  
  


  
  
  
**Limited Contention Protocols:**

* + - Collision based protocols (pure and slotted ALOHA, CSMA/CD) are good when the network load is low.
    - Collision free protocols (bitmap, binary Countdown) are good when load is high.
    - How about combining their advantages
      1. Behave like the ALOHA scheme under light load
      2. Behave like the bitmap scheme under heavy load.

**Adaptive Tree Walk Protocol:**

* + - 1. partition the gro
      2. up of station and limit the contention for each slot.

Under light load, everyone can try for each slot like aloha

* + - 1. Under heavy load, only a group can try for each slot
      2. **How do we do it:**
         1. treat every stations as the leaf of a binary tree
         2. first slot (after successful transmission), all stations  
            can try to get the slot(under the root node).
         3. if no conflict, fine
         4. in case of conflict, only nodes under a subtree get to try for the next one. (depth first search)

**For Example:**

* + - 1. **Slot-0:** C\*, E\*, F\*, H\* (all nodes under node 0 can try which are going to send), conflict
      2. **Slot-1:** C\* (all nodes under node 1can try}, C sends
      3. **Slot-2:** E\*, F\*, H\*(all nodes under node 2 can try}, conflict
      4. **Slot-3:** E\*, F\* (all nodes under node 5 can try to send), conflict
      5. **Slot-4:** E\* (all nodes under E can try), E sends
      6. **Slot-5:** F\* (all nodes under F can try), F sends
      7. **Slot-6:** H\* (all nodes under node 6 can try to send), H sends.

**This unit is not completed yet**