Unit 3

B230503T Data and Communication Networks

Multiplexing, error detection and correction: Many to one, one to many, WDM, TDM, FDM, Circuit switching, packet switching and message switching. Data link control protocols: Line discipline, flow control, error control, synchronous and asynchronous protocols, Character and bit oriented protocols, Link access procedures. Point to point controls: Transmission states, PPP layers, I-CP. Authentication, NCP.ISDN: Services, Historical outline, subscriber's access, ISDN Layers and broadcast ISDN.

Multiplexing:
Multiplexing is a technique used to combine and send the multiple data streams over a single medium. The process of combining the data st reams is known as multiplexing and hardware used for multiplexing is known as a multiplexer.
Multiplexing is achieved by using a device called Multiplexer (MUX) that combines n input lines to generate a single output line. Multiplexing follows many-to-one, i.e., n input lines and one output line.

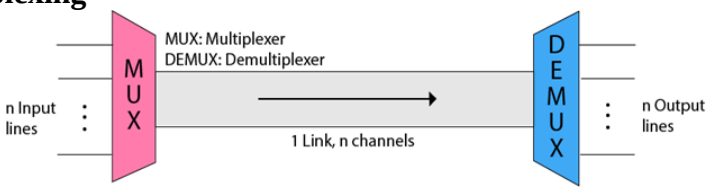
Demultiplexing:
Demultiplexing is achieved by using a device called Demultiplexer (DEMUX) available at the receiving end. DEMUX separates a signal into its component signals (one input and n outputs). Therefore, we can say that demultiplexing follows the one-to-many approach.

Why Multiplexing?
The transmission medium is used to send the signal from sender to receiver. The medium can only have one signal at a time.
If there are multiple signals to share one medium, then the medium must be divided in such a way that each signal is given some portion of the available bandwidth. For example: If there are 10 signals and bandwidth of medium is100 units, then the 10 unit is shared by each signal.

- When multiple signals share the common medium, there is a possibility of collision? Multiplexing concept is used to avoid such collision.
- Transmission services are very expensive.

History of Multiplexing
Multiplexing technique is widely used in telecommunications in which several telephone calls are carried through a single wire.
Multiplexing originated in telegraphy in the early 1870s and is now widely used in communication.
George Owen Squier developed the telephone carrier multiplexing in 1910.

Concept of Multiplexing



The 'n' input lines are transmitted through a multiplexer and multiplexer combines the signals to form a composite signal.
The composite signal is passed through a Demultiplexer and demultiplexer separates a signal to component signals and transfers them to their respective destinations.

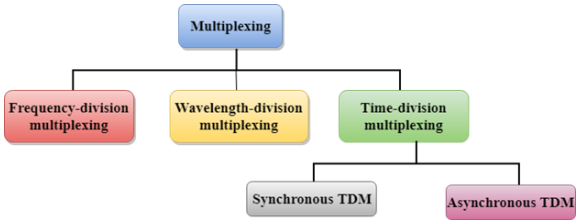
Advantages of Multiplexing:

- More than one signal can be sent over a single medium.

- The bandwidth of a medium can be utilized effectively.
- Multiplexing Techniques
- Multiplexing techniques can be classified as:

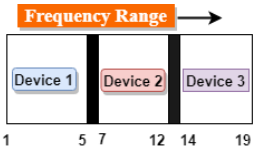
Multiplexing Techniques:

Multiplexing techniques can be classified as:

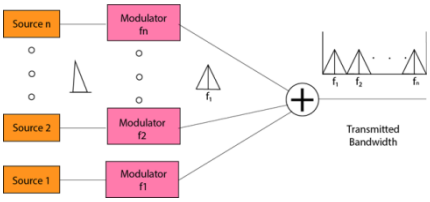


Frequency-division Multiplexing (FDM)

- It is an analog technique.
- **Frequency Division Multiplexing** is a technique in which the available bandwidth of a single transmission medium is subdivided into several channels.



- In the above diagram, a single transmission medium is subdivided into several frequency channels, and each frequency channel is given to different devices. Device 1 has a frequency channel of range from 1 to 5.
- The input signals are translated into frequency bands by using modulation techniques, and they are combined by a multiplexer to form a composite signal.
- The main aim of the FDM is to subdivide the available bandwidth into different frequency channels and allocate them to different devices.
- Using the modulation technique, the input signals are transmitted into frequency bands and then combined to form a composite signal.
- The carriers which are used for modulating the signals are known as **sub-carriers**. They are represented as f1,f2..fn.
- **FDM** is mainly used in radio broadcasts and TV networks.



Advantages of FDM:

- FDM is used for analog signals.
- FDM process is very simple and easy modulation.
- A Large number of signals can be sent through an FDM simultaneously.
- It does not require any synchronization between sender and receiver.

Disadvantages of FDM:

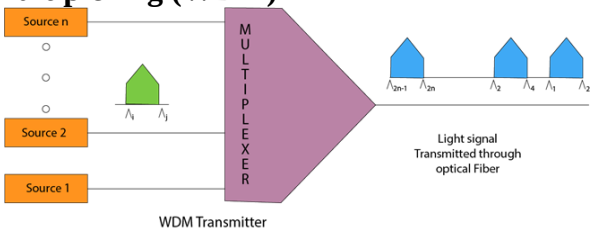
- FDM technique is used only when low-speed channels are required.
- It suffers the problem of crosstalk.
- A Large number of modulators are required.
- It requires a high bandwidth channel.

Applications of FDM:

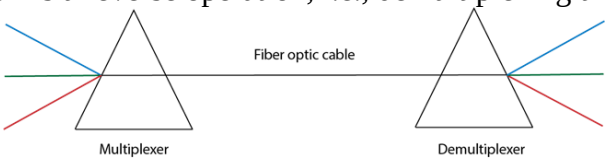
- FDM is commonly used in TV networks.

- It is used in FM and AM broadcasting. Each FM radio station has different frequencies, and they are multiplexed to form a composite signal. The multiplexed signal is transmitted in the air.

Wavelength Division Multiplexing (WDM)



- Wavelength Division Multiplexing is same as FDM except that the optical signals are transmitted through the fibre optic cable.
- WDM is used on fibre optics to increase the capacity of a single fibre.
- It is used to utilize the high data rate capability of fibre optic cable.
- It is an analog multiplexing technique.
- Optical signals from different source are combined to form a wider band of light with the help of multiplexer.
- At the receiving end, demultiplexer separates the signals to transmit them to their respective destinations.
- Multiplexing and Demultiplexing can be achieved by using a prism.
- Prism can perform a role of multiplexer by combining the various optical signals to form a composite signal, and the composite signal is transmitted through a fibre optical cable.
- Prism also performs a reverse operation, i.e., demultiplexing the signal.



Time Division Multiplexing

- It is a digital technique.
- In Frequency Division Multiplexing Technique, all signals operate at the same time with different frequency, but in case of Time Division Multiplexing technique, all signals operate at the same frequency with different time.
- In **Time Division Multiplexing technique**, the total time available in the channel is distributed among different users. Therefore, each user is allocated with different time interval known as a Time slot at which data is to be transmitted by the sender.
- A user takes control of the channel for a fixed amount of time.
- In Time Division Multiplexing technique, data is not transmitted simultaneously rather the data is transmitted one-by-one.
- In TDM, the signal is transmitted in the form of frames. Frames contain a cycle of time slots in which each frame contains one or more slots dedicated to each user.
- It can be used to multiplex both digital and analog signals but mainly used to multiplex digital signals.

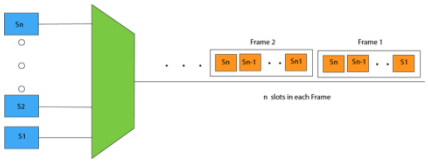
There are two types of TDM:

- Synchronous TDM
- Asynchronous TDM

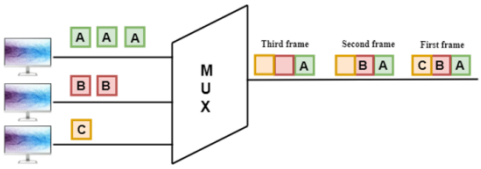
Synchronous TDM

- A Synchronous TDM is a technique in which time slot is preassigned to every device.

- In Synchronous TDM, each device is given some time slot irrespective of the fact that the device contains the data or not.
- If the device does not have any data, then the slot will remain empty.
- In Synchronous TDM, signals are sent in the form of frames. Time slots are organized in the form of frames. If a device does not have data for a particular time slot, then the empty slot will be transmitted.
- The most popular Synchronous TDM are T-1 multiplexing, ISDN multiplexing, and SONET multiplexing.
- If there are n devices, then there are n slots.



Concept of Synchronous TDM



In the above figure, the Synchronous TDM technique is implemented. Each device is allocated with some time slot. The time slots are transmitted irrespective of whether the sender has data to send or not.

Disadvantages of Synchronous TDM:

- The capacity of the channel is not fully utilized as the empty slots are also transmitted which is having no data. In the above figure, the first frame is completely filled, but in the last two frames, some slots are empty. Therefore, we can say that the capacity of the channel is not utilized efficiently.
- The speed of the transmission medium should be greater than the total speed of the input lines. An alternative approach to the Synchronous TDM is Asynchronous Time Division Multiplexing.

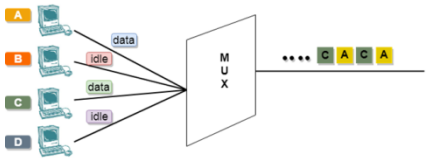
Asynchronous TDM

- An asynchronous TDM is also known as Statistical TDM.
- An asynchronous TDM is a technique in which time slots are not fixed as in the case of Synchronous TDM. Time slots are allocated to only those devices which have the data to send. Therefore, we can say that Asynchronous Time Division multiplexor transmits only the data from active workstations.
- An asynchronous TDM technique dynamically allocates the time slots to the devices.
- In Asynchronous TDM, total speed of the input lines can be greater than the capacity of the channel.
- Asynchronous Time Division multiplexor accepts the incoming data streams and creates a frame that contains only data with no empty slots.
- In Asynchronous TDM, each slot contains an address part that identifies the source of the data.

- The difference between Asynchronous TDM and Synchronous TDM is that many slots in Synchronous TDM are unutilized, but in Asynchronous TDM, slots are fully utilized. This leads to the smaller transmission time and efficient utilization of the capacity of the channel.

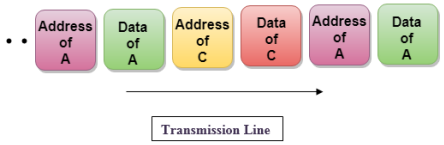
- In Synchronous TDM, if there are n sending devices, then there are n time slots. In Asynchronous TDM, if there are n sending devices, then there are m time slots where m is less than n (**m<n**).
- The number of slots in a frame depends on the statistical analysis of the number of input lines.

Concept of Asynchronous TDM



In the above diagram, there are 4 devices, but only two devices are sending the data, i.e., A and C. Therefore, the data of A and C are only transmitted through the transmission line.

Frame of above diagram can be represented as:

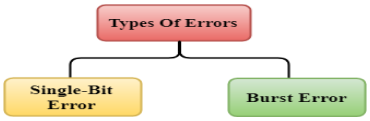


The above figure shows that the data part contains the address to determine the source of the data.

Error Detection

When data is transmitted from one device to another device, the system does not guarantee whether the data received by the device is identical to the data transmitted by another device. An Error is a situation when the message received at the receiver end is not identical to the message transmitted.

Types of Errors

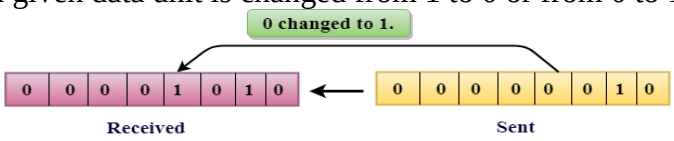


Errors can be classified into two categories:

- Single-Bit Error
- Burst Error

Single-Bit Error:

The only one bit of a given data unit is changed from 1 to 0 or from 0 to 1.



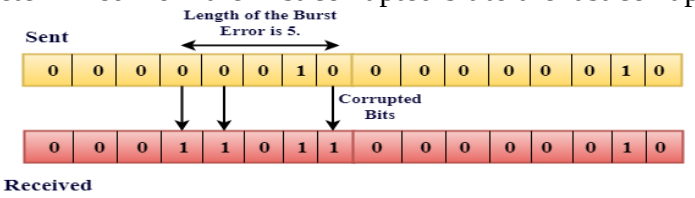
In the above figure, the message which is sent is corrupted as single-bit, i.e., 0 bit is changed to 1.

Single-Bit Error does not appear more likely in Serial Data Transmission. For example, Sender sends the data at 10 Mbps, this means that the bit lasts only for 1 ?s and for a single-bit error to occurred, a noise must be more than 1 ?s.

Single-Bit Error mainly occurs in Parallel Data Transmission. For example, if eight wires are used to send the eight bits of a byte, if one of the wire is noisy, then single-bit is corrupted per byte.

Burst Error:

The two or more bits are changed from 0 to 1 or from 1 to 0 is known as Burst Error.
The Burst Error is determined from the first corrupted bit to the last corrupted bit.



The duration of noise in Burst Error is more than the duration of noise in Single-Bit.
Burst Errors are most likely to occur in Serial Data Transmission.
The number of affected bits depends on the duration of the noise and data rate.

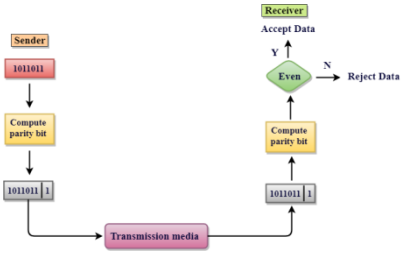
Error Detecting Techniques:

The most popular Error Detecting Techniques are:

- Single parity check
- Two-dimensional parity check
- Checksum
- Cyclic redundancy check

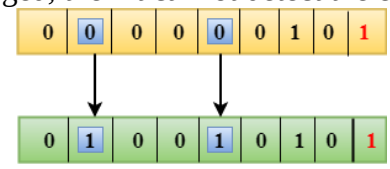
Single Parity Check

- Single Parity checking is the simple mechanism and inexpensive to detect the errors.
- In this technique, a redundant bit is also known as a parity bit which is appended at the end of the data unit so that the number of 1s becomes even. Therefore, the total number of transmitted bits would be 9 bits.
- If the number of 1s bits is odd, then parity bit 1 is appended and if the number of 1s bits is even, then parity bit 0 is appended at the end of the data unit.
- At the receiving end, the parity bit is calculated from the received data bits and compared with the received parity bit.
- This technique generates the total number of 1s even, so it is known as even-parity checking.



Drawbacks of Single Parity Checking

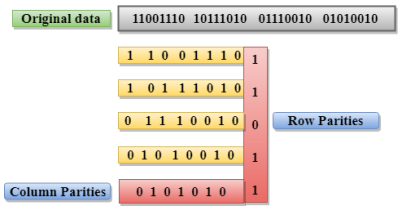
- It can only detect single-bit errors which are very rare.
- If two bits are interchanged, then it cannot detect the errors.



Two-Dimensional Parity Check

- Performance can be improved by using **Two-Dimensional Parity Check** which organizes the data in the form of a table.
- Parity check bits are computed for each row, which is equivalent to the single-parity check.
- In Two-Dimensional Parity check, a block of bits is divided into rows, and the redundant row of bits is added to the whole block.

- At the receiving end, the parity bits are compared with the parity bits computed from the received data.



Drawbacks of 2D Parity Check

- If two bits in one data unit are corrupted and two bits exactly the same position in another data unit are also corrupted, then 2D Parity checker will not be able to detect the error.
- This technique cannot be used to detect the 4-bit errors or more in some cases.

Checksum

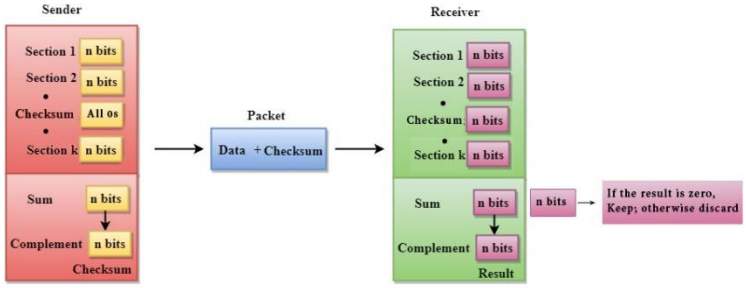
A Checksum is an error detection technique based on the concept of redundancy.

It is divided into two parts:

Checksum Generator

A Checksum is generated at the sending side. Checksum generator subdivides the data into equal segments of n bits each, and all these segments are added together by using one's complement arithmetic. The sum is complemented and appended to the original data, known as checksum field. The extended data is transmitted across the network.

Suppose L is the total sum of the data segments, then the checksum would be ?L



The Sender follows the given steps:

1. The block unit is divided into k sections, and each of n bits.
2. All the k sections are added together by using one's complement to get the sum.
3. The sum is complemented and it becomes the checksum field.
4. The original data and checksum field are sent across the network.

Checksum Checker

A Checksum is verified at the receiving side. The receiver subdivides the incoming data into equal segments of n bits each, and all these segments are added together, and then this sum is complemented. If the complement of the sum is zero, then the data is accepted otherwise data is rejected.

1. The Receiver follows the given steps:
2. The block unit is divided into k sections and each of n bits.
3. All the k sections are added together by using one's complement algorithm to get the sum.
4. The sum is complemented.
5. If the result of the sum is zero, then the data is accepted otherwise the data is discarded.

Cyclic Redundancy Check (CRC)

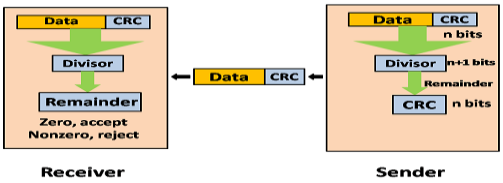
CRC is a redundancy error technique used to determine the error.

Following are the steps used in CRC for error detection:

- In CRC technique, a string of n 0s is appended to the data unit, and this n number is less than the number of bits in a predetermined number, known as division which is n+1 bits.
- Secondly, the newly extended data is divided by a divisor using a process is known as binary division. The remainder generated from this division is known as CRC remainder.
- Thirdly, the CRC remainder replaces the appended 0s at the end of the original data. This newly generated unit is sent to the receiver.
- The receiver receives the data followed by the CRC remainder. The receiver will treat this whole unit as a single unit, and it is divided by the same divisor that was used to find the CRC remainder.

If the resultant of this division is zero which means that it has no error, and the data is accepted.

If the resultant of this division is not zero which means that the data consists of an error. Therefore, the data is discarded.

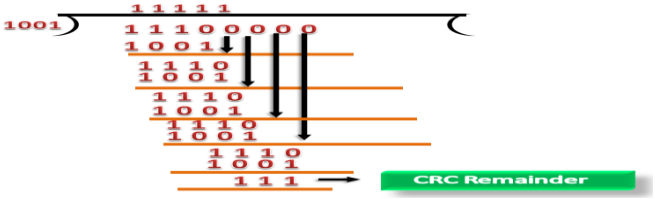


Let's understand this concept through an example:

Suppose the original data is 11100 and divisor is 1001.

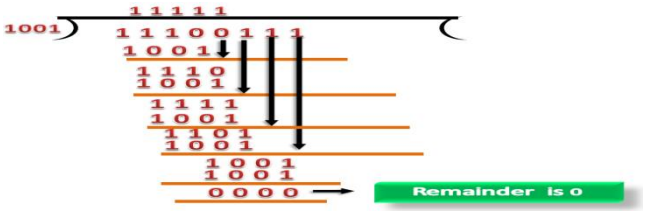
CRC Generator

- A CRC generator uses a modulo-2 division. Firstly, three zeroes are appended at the end of the data as the length of the divisor is 4 and we know that the length of the string 0s to be appended is always one less than the length of the divisor.
- Now, the string becomes 11100000, and the resultant string is divided by the divisor 1001.
- The remainder generated from the binary division is known as CRC remainder. The generated value of the CRC remainder is 111.
- CRC remainder replaces the appended string of 0s at the end of the data unit, and the final string would be 11100111 which is sent across the network.



CRC Checker

- The functionality of the CRC checker is similar to the CRC generator.
- When the string 11100111 is received at the receiving end, then CRC checker performs the modulo-2 division.
- A string is divided by the same divisor, i.e., 1001.
- In this case, CRC checker generates the remainder of zero. Therefore, the data is accepted.



Error Correction

Error Correction codes are used to detect and correct the errors when data is transmitted from the sender to the receiver.

Error Correction can be handled in two ways:

- **Backward error correction:** Once the error is discovered, the receiver requests the sender to retransmit the entire data unit.
- **Forward error correction:** In this case, the receiver uses the error-correcting code which automatically corrects the errors.

A single additional bit can detect the error, but cannot correct it.

For correcting the errors, one has to know the exact position of the error. For example, If we want to calculate a single-bit error, the error correction code will determine which one of seven bits is in error. To achieve this, we have to add some additional redundant bits.

Suppose r is the number of redundant bits and d is the total number of the data bits. The number of redundant bits r can be calculated by using the formula:

$2^r >= d+r+1$

The value of r is calculated by using the above formula. For example, if the value of d is 4, then the possible smallest value that satisfies the above relation would be 3.

To determine the position of the bit which is in error, a technique developed by R.W Hamming is Hamming code which can be applied to any length of the data unit and uses the relationship between data units and redundant units.

Hamming Code

Parity bits: The bit which is appended to the original data of binary bits so that the total number of 1s is even or odd.

Even parity: To check for even parity, if the total number of 1s is even, then the value of the parity bit is 0. If the total number of 1s occurrences is odd, then the value of the parity bit is 1.

Odd Parity: To check for odd parity, if the total number of 1s is even, then the value of parity bit is 1. If the total number of 1s is odd, then the value of parity bit is 0.

Algorithm of Hamming code:

- An information of 'd' bits are added to the redundant bits 'r' to form d+r.
- The location of each of the (d+r) digits is assigned a decimal value.
- The 'r' bits are placed in the positions $1,2,.....2^{k-1}$.
- At the receiving end, the parity bits are recalculated. The decimal value of the parity bits determines the position of an error.
-

Relationship b/w Error position & binary number.

Error Position	Binary Number
0	000
1	001
2	010
3	011
4	100
5	101
6	110
7	111

Let's understand the concept of Hamming code through an example:

Suppose the original data is 1010 which is to be sent.

otal number of data bits 'd' = 4

Number of redundant bits r : $2^r >= d+r+1$

$2^r >= 4+r+1$

Therefore, the value of r is 3 that satisfies the above relation.

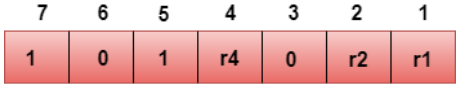
Total number of bits = d+r = 4+3 = 7;

Determining the position of the redundant bits

The number of redundant bits is 3. The three bits are represented by r1, r2, r4. The position of the redundant bits is calculated with corresponds to the raised power of 2. Therefore, their corresponding positions are **1, 2^1, 2^2**.

1. The position of r1 = 1
2. The position of r2 = 2
3. The position of r4 = 4

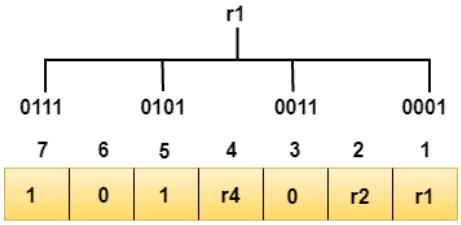
Representation of Data on the addition of parity bits:



Determining the Parity bits

Determining the r1 bit

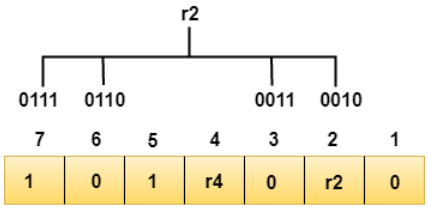
The r1 bit is calculated by performing a parity check on the bit positions whose binary representation includes 1 in the first position.



We observe from the above figure that the bit positions that includes 1 in the first position are 1, 3, 5, 7. Now, we perform the even-parity check at these bit positions. The total number of 1 at these bit positions corresponding to r1 is **even, therefore, the value of the r1 bit is 0**.

Determining r2 bit

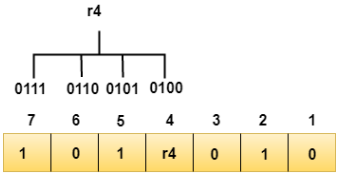
The r2 bit is calculated by performing a parity check on the bit positions whose binary representation includes 1 in the second position.



We observe from the above figure that the bit positions that includes 1 in the second position are **2, 3, 6, 7**. Now, we perform the even-parity check at these bit positions. The total number of 1 at these bit positions corresponding to r2 is **odd, therefore, the value of the r2 bit is 1**.

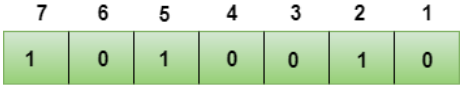
Determining r4 bit

The r4 bit is calculated by performing a parity check on the bit positions whose binary representation includes 1 in the third position.



We observe from the above figure that the bit positions that includes 1 in the third position are **4, 5, 6, 7**. Now, we perform the even-parity check at these bit positions. The total number of 1 at these bit positions corresponding to r4 is **even, therefore, the value of the r4 bit is 0**.

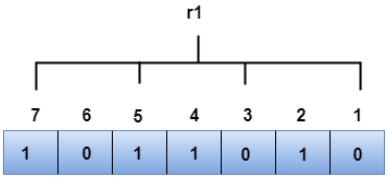
Data transferred is given below:



Suppose the 4th bit is changed from 0 to 1 at the receiving end, then parity bits are recalculated.

R1 bit

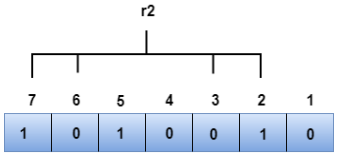
The bit positions of the r1 bit are 1,3,5,7



We observe from the above figure that the binary representation of r1 is 1100. Now, we perform the even-parity check, the total number of 1s appearing in the r1 bit is an even number. Therefore, the value of r1 is 0.

R2 bit

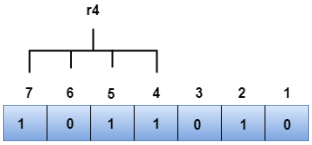
The bit positions of r2 bit are 2,3,6,7.



We observe from the above figure that the binary representation of r2 is 1001. Now, we perform the even-parity check, the total number of 1s appearing in the r2 bit is an even number. Therefore, the value of r2 is 0.

R4 bit

The bit positions of r4 bit are 4,5,6,7.



We observe from the above figure that the binary representation of r4 is 1011. Now, we perform the even-parity check, the total number of 1s appearing in the r4 bit is an odd number. Therefore, the value of r4 is 1.

- The binary representation of redundant bits, i.e., r4r2r1 is 100, and its corresponding decimal value is 4. Therefore, the error occurs in a 4th bit position. The bit value must be changed from 1 to 0 to correct the error.

Switching

- When a user accesses the internet or another computer network outside their immediate location, messages are sent through the network of transmission media. This technique of transferring the information from one computer network to another network is known as **switching**.
- Switching in a computer network is achieved by using switches. A switch is a small hardware device which is used to join multiple computers together with one local area network (LAN).
- Network switches operate at layer 2 (Data link layer) in the OSI model.

- Switching is transparent to the user and does not require any configuration in the home network.
- Switches are used to forward the packets based on MAC addresses.
- A Switch is used to transfer the data only to the device that has been addressed. It verifies the destination address to route the packet appropriately.
- It is operated in full duplex mode.
- Packet collision is minimum as it directly communicates between source and destination.
- It does not broadcast the message as it works with limited bandwidth.

Why is Switching Concept required?

Switching concept is developed because of the following reasons:

- **Bandwidth:** It is defined as the maximum transfer rate of a cable. It is a very critical and expensive resource. Therefore, switching techniques are used for the effective utilization of the bandwidth of a network.
- **Collision:** Collision is the effect that occurs when more than one device transmits the message over the same physical media, and they collide with each other. To overcome this problem, switching technology is implemented so that packets do not collide with each other.

Advantages of Switching:

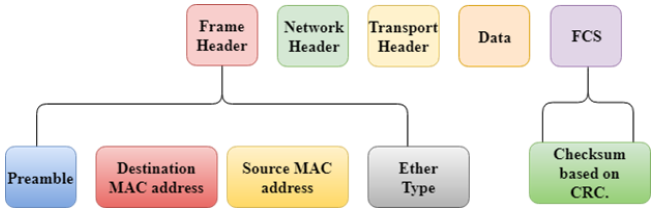
- Switch increases the bandwidth of the network.
- It reduces the workload on individual PCs as it sends the information to only that device which has been addressed.
- It increases the overall performance of the network by reducing the traffic on the network.
- There will be less frame collision as switch creates the collision domain for each connection.

Disadvantages of Switching:

- A Switch is more expensive than network bridges.
- A Switch cannot determine the network connectivity issues easily.
- Proper designing and configuration of the switch are required to handle multicast packets.

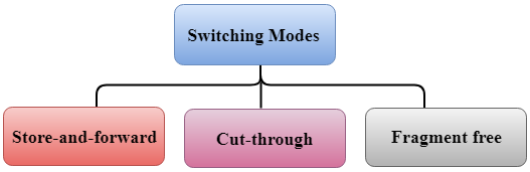
Switching Modes

- The layer 2 switches are used for transmitting the data on the data link layer, and it also performs error checking on transmitted and received frames.
- The layer 2 switches forward the packets with the help of MAC address.
- Different modes are used for forwarding the packets known as **Switching modes**.
- In **switching mode**, Different parts of a frame are recognized. The frame consists of several parts such as preamble, destination MAC address, source MAC address, user's data, FCS.



There are three types of switching modes:

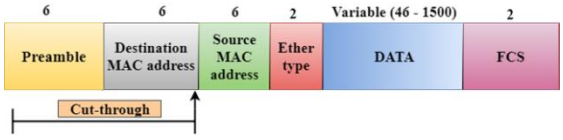
- Store-and-forward
- Cut-through
- Fragment-free



Store-and-forward

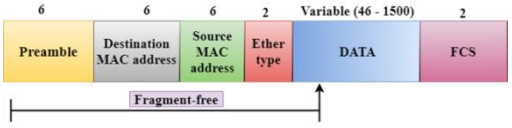
- Store-and-forward is a technique in which the intermediate nodes store the received frame and then check for errors before forwarding the packets to the next node.
- The layer 2 switch waits until the entire frame has received. On receiving the entire frame, switch store the frame into the switch buffer memory. This process is known as **storing the frame**.
- When the frame is stored, then the frame is checked for the errors. If any error found, the message is discarded otherwise the message is forwarded to the next node. This process is known as **forwarding the frame**.
- CRC (Cyclic Redundancy Check) technique is implemented that uses a number of bits to check for the errors on the received frame.
- The store-and-forward technique ensures a high level of security as the destination network will not be affected by the corrupted frames.
- Store-and-forward switches are highly reliable as it does not forward the collided frames.

Cut-through Switching



- Cut-through switching is a technique in which the switch forwards the packets after the destination address has been identified without waiting for the entire frame to be received.
- Once the frame is received, it checks the first six bytes of the frame following the preamble, the switch checks the destination in the switching table to determine the outgoing interface port, and forwards the frame to the destination.
- It has **low latency** rate as the switch does not wait for the entire frame to be received before sending the packets to the destination.
- It has no **error checking technique**. Therefore, the errors can be sent with or without errors to the receiver.
- A Cut-through switching technique has **low wait time** as it forwards the packets as soon as it identifies the destination MAC address.
- In this technique, collision is not detected, if frames have collided will also be forwarded.

Fragment-free Switching



- A Fragment-free switching is an advanced technique of the Cut-through Switching.

- A Fragment-free switching is a technique that reads atleast 64 bytes of a frame before forwarding to the next node to provide the error-free transmission.
- It combines the speed of Cut-through Switching with the error checking functionality.
- This technique checks the 64 bytes of the ethernet frame where addressing information is available.
- A collision is detected within 64 bytes of the frame, the frames which are collided will not be forwarded further.

Differences b/w Store-and-forward and Cut-through Switching.

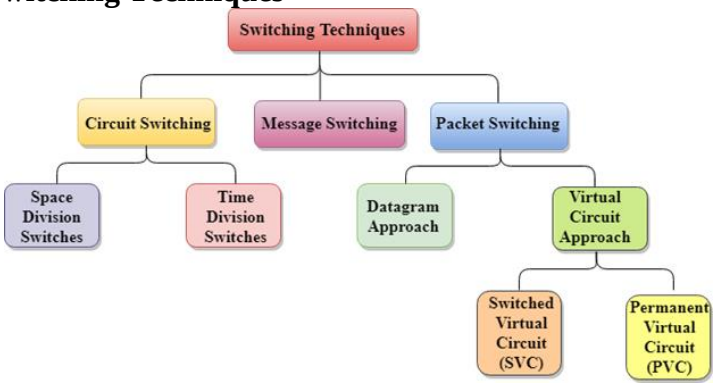
Store-and-forward Switching	Cut-through Switching
Store-and-forward Switching is a technique that waits until the entire frame is received.	Cut-through Switching is a technique that checks the first 6 bytes following the preamble to identify the destination address.
It performs error checking functionality. If any error is found in the frame, the frame will be discarded otherwise forwarded to the next node.	It does not perform any error checking. The frame with or without errors will be forwarded.
It has high latency rate as it waits for the entire frame to be received before forwarding to the next node.	It has low latency rate as it checks only six bytes of the frame to determine the destination address.
It is highly reliable as it forwards only error-free packets.	It is less reliable as compared to Store-and-forward technique as it forwards error prone packets as well.
It has a high wait time as it waits for the entire frame to be received before taking any forwarding decisions.	It has low wait time as cut-through switches do not store the whole frame or packets.

Switching techniques

In large networks, there can be multiple paths from sender to receiver. The switching technique will decide the best route for data transmission.

Switching technique is used to connect the systems for making one-to-one communication.

Classification of Switching Techniques

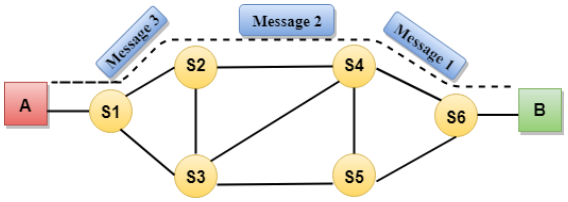


Circuit Switching

- Circuit switching is a switching technique that establishes a dedicated path between sender and receiver.
- In the Circuit Switching Technique, once the connection is established then the dedicated path will remain to exist until the connection is terminated.
- Circuit switching in a network operates in a similar way as the telephone works.
- A complete end-to-end path must exist before the communication takes place.
- In case of circuit switching technique, when any user wants to send the data, voice, video, a request signal is sent to the receiver then the receiver sends back the acknowledgment to ensure the availability of the dedicated path. After receiving the acknowledgment, dedicated path transfers the data.
- Circuit switching is used in public telephone network. It is used for voice transmission.
- Fixed data can be transferred at a time in circuit switching technology.

Communication through circuit switching has 3 phases:

- Circuit establishment
- Data transfer
- Circuit Disconnect



Circuit Switching can use either of the two technologies:

Space Division Switches:

- Space Division Switching is a circuit switching technology in which a single transmission path is accomplished in a switch by using a physically separate set of cross points.
- Space Division Switching can be achieved by using crossbar switch. A crossbar switch is a metallic cross point or semiconductor gate that can be enabled or disabled by a control unit.
- The Crossbar switch is made by using the semiconductor. For example, Xilinx crossbar switches using FPGAs.
- Space Division Switching has high speed, high capacity, and nonblocking switches.

Space Division Switches can be categorized in two ways:

- **Crossbar Switch**
- **Multistage Switch**

Crossbar Switch

The Crossbar switch is a switch that has n input lines and n output lines. The crossbar switch has n^2 intersection points known as **cross points.**

Disadvantage of Crossbar switch:

The number of cross points increases as the number of stations is increased. Therefore, it becomes very expensive for a large switch. The solution to this is to use a multistage switch.

Multistage Switch

- Multistage Switch is made by splitting the crossbar switch into the smaller units and then interconnecting them.
- It reduces the number of cross points.
- If one path fails, then there will be an availability of another path.

Advantages of Circuit Switching:

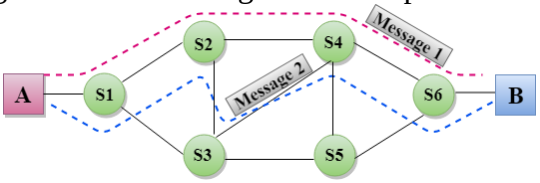
- In the case of Circuit Switching technique, the communication channel is dedicated.
- It has fixed bandwidth.

Disadvantages of Circuit Switching:

- Once the dedicated path is established, the only delay occurs in the speed of data transmission.
- It takes a long time to establish a connection approx 10 seconds during which no data can be transmitted.
- It is more expensive than other switching techniques as a dedicated path is required for each connection.
- It is inefficient to use because once the path is established and no data is transferred, then the capacity of the path is wasted.
- In this case, the connection is dedicated therefore no other data can be transferred even if the channel is free.

Message Switching

- Message Switching is a switching technique in which a message is transferred as a complete unit and routed through intermediate nodes at which it is stored and forwarded.
- In Message Switching technique, there is no establishment of a dedicated path between the sender and receiver.
- The destination address is appended to the message. Message Switching provides a dynamic routing as the message is routed through the intermediate nodes based on the information available in the message.
- Message switches are programmed in such a way so that they can provide the most efficient routes.
- Each and every node stores the entire message and then forward it to the next node. This type of network is known as **store and forward network.**
- Message switching treats each message as an independent entity.



Advantages of Message Switching

- Data channels are shared among the communicating devices that improve the efficiency of using available bandwidth.
- Traffic congestion can be reduced because the message is temporarily stored in the nodes.
- Message priority can be used to manage the network.
- The size of the message which is sent over the network can be varied. Therefore, it supports the data of unlimited size.

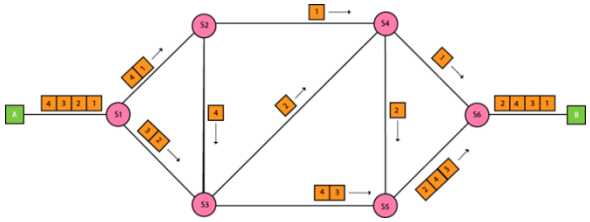
Disadvantages of Message Switching

- The message switches must be equipped with sufficient storage to enable them to store the messages until the message is forwarded.
- The Long delay can occur due to the storing and forwarding facility provided by the message switching technique.

Packet Switching

- The packet switching is a switching technique in which the message is sent in one go, but it is divided into smaller pieces, and they are sent individually.

- The message splits into smaller pieces known as packets and packets are given a unique number to identify their order at the receiving end.
- Every packet contains some information in its headers such as source address, destination address and sequence number.
- Packets will travel across the network, taking the shortest path as possible.
- All the packets are reassembled at the receiving end in correct order.
- If any packet is missing or corrupted, then the message will be sent to resend the message.
- If the correct order of the packets is reached, then the acknowledgment message will be sent.



Approaches of Packet Switching:

There are two approaches to Packet Switching:

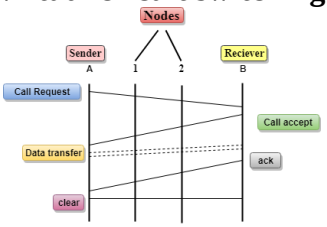
Datagram Packet Switching:

- It is a packet switching technology in which packet is known as a datagram, is considered as an independent entity. Each packet contains the information about the destination and switch uses this information to forward the packet to the correct destination.
- The packets are reassembled at the receiving end in correct order.
- In Datagram Packet Switching technique, the path is not fixed.
- Intermediate nodes take the routing decisions to forward the packets.
- Datagram Packet Switching is also known as connectionless switching.

Virtual Circuit Switching:

- Virtual Circuit Switching is also known as connection-oriented switching.
- In the case of Virtual circuit switching, a preplanned route is established before the messages are sent.
- Call request and call accept packets are used to establish the connection between sender and receiver.
- In this case, the path is fixed for the duration of a logical connection.

Let's understand the concept of virtual circuit switching through a diagram:



- In the above diagram, A and B are the sender and receiver respectively. 1 and 2 are the nodes.
- Call request and call accept packets are used to establish a connection between the sender and receiver.
- When a route is established, data will be transferred.
- After transmission of data, an acknowledgment signal is sent by the receiver that the message has been received.
- If the user wants to terminate the connection, a clear signal is sent for the termination.

Differences b/w Datagram approach and Virtual Circuit approach

Datagram approach	Virtual Circuit approach
Node takes routing decisions to forward the packets.	Node does not take any routing decision.
Congestion cannot occur as all the packets travel in different directions.	Congestion can occur when the node is busy, and it does not allow other packets to pass through.
It is more flexible as all the packets are treated as an independent entity.	It is not very flexible.

Advantages of Packet Switching:

- **Cost-effective:** In packet switching technique, switching devices do not require massive secondary storage to store the packets, so cost is minimized to some extent. Therefore, we can say that the packet switching technique is a cost-effective technique.
- **Reliable:** If any node is busy, then the packets can be rerouted. This ensures that the Packet Switching technique provides reliable communication.
- **Efficient:** Packet Switching is an efficient technique. It does not require any established path prior to the transmission, and many users can use the same communication channel simultaneously, hence makes use of available bandwidth very efficiently.

Disadvantages of Packet Switching:

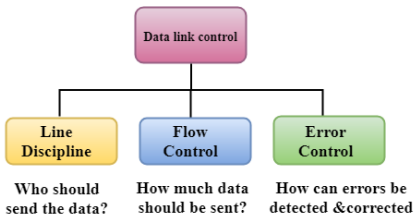
- Packet Switching technique cannot be implemented in those applications that require low delay and high-quality services.
- The protocols used in a packet switching technique are very complex and requires high implementation cost.
- If the network is overloaded or corrupted, then it requires retransmission of lost packets. It can also lead to the loss of critical information if errors are nor recovered.

Data Link Controls

Data Link Control is the service provided by the Data Link Layer to provide reliable data transfer over the physical medium. For example, In the half-duplex transmission mode, one device can only transmit the data at a time. If both the devices at the end of the links transmit the data simultaneously, they will collide and leads to the loss of the information. The Data link layer provides the coordination among the devices so that no collision occurs.

The Data link layer provides three functions:

- Line discipline
- Flow Control
- Error Control



Line Discipline:

- Line Discipline is a functionality of the Data link layer that provides the coordination among the link systems. It determines which device can send, and when it can send the data.

Line Discipline can be achieved in two ways:

- ENQ/ACK
- Poll/select

END/ACK

END/ACK stands for Enquiry/Acknowledgement is used when there is no wrong receiver available on the link and having a dedicated path between the two devices so that the device capable of receiving the transmission is the intended one.

END/ACK coordinates which device will start the transmission and whether the recipient is ready or not.

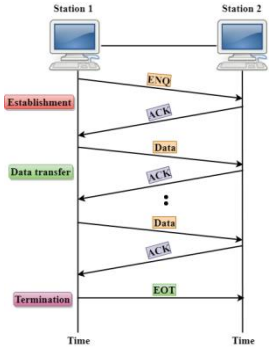
Working of END/ACK

The transmitter transmits the frame called an Enquiry (ENQ) asking whether the receiver is available to receive the data or not.

The receiver responses either with the positive acknowledgement(ACK) or with the negative acknowledgement(NACK) where positive acknowledgement means that the receiver is ready to receive the transmission and negative acknowledgement means that the receiver is unable to accept the transmission.

Following are the responses of the receiver:

- If the response to the ENQ is positive, the sender will transmit its data, and once all of its data has been transmitted, the device finishes its transmission with an EOT (END-of-Transmission) frame.
- If the response to the ENQ is negative, then the sender disconnects and restarts the transmission at another time.
- If the response is neither negative nor positive, the sender assumes that the ENQ frame was lost during the transmission and makes three attempts to establish a link before giving up.



Poll/Select

The Poll/Select method of line discipline works with those topologies where one device is designated as a primary station, and other devices are secondary stations.

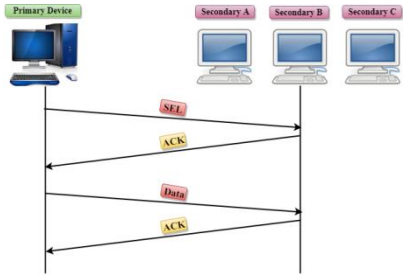
Working of Poll/Select

- In this, the primary device and multiple secondary devices consist of a single transmission line, and all the exchanges are made through the primary device even though the destination is a secondary device.
- The primary device has control over the communication link, and the secondary device follows the instructions of the primary device.
- The primary device determines which device is allowed to use the communication channel. Therefore, we can say that it is an initiator of the session.

- If the primary device wants to receive the data from the secondary device, it asks the secondary device that they anything to send, this process is known as polling.
- If the primary device wants to send some data to the secondary device, then it tells the target secondary to get ready to receive the data, this process is known as selecting.

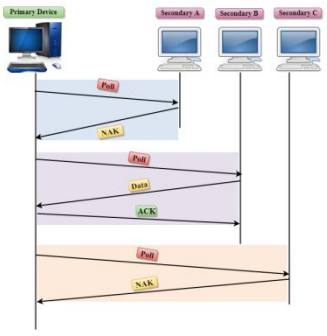
Select

- The select mode is used when the primary device has something to send.
- When the primary device wants to send some data, then it alerts the secondary device for the upcoming transmission by transmitting a Select (SEL) frame, one field of the frame includes the address of the intended secondary device.
- When the secondary device receives the SEL frame, it sends an acknowledgement that indicates the secondary ready status.
- If the secondary device is ready to accept the data, then the primary device sends two or more data frames to the intended secondary device. Once the data has been transmitted, the secondary sends an acknowledgement specifies that the data has been received.



Poll

- The Poll mode is used when the primary device wants to receive some data from the secondary device.
- When a primary device wants to receive the data, then it asks each device whether it has anything to send.
- Firstly, the primary asks (poll) the first secondary device, if it responds with the NACK (Negative Acknowledgement) means that it has nothing to send. Now, it approaches the second secondary device, it responds with the ACK means that it has the data to send. The secondary device can send more than one frame one after another or sometimes it may be required to send ACK before sending each one, depending on the type of the protocol being used.



Flow Control

- It is a set of procedures that tells the sender how much data it can transmit before the data overwhelms the receiver.
- The receiving device has limited speed and limited memory to store the data. Therefore, the receiving device must be able to inform the sending device to stop the transmission temporarily before the limits are reached.

- It requires a buffer, a block of memory for storing the information until they are processed.

Two methods have been developed to control the flow of data:

- Stop-and-wait
- Sliding window

Stop-and-wait

- In the Stop-and-wait method, the sender waits for an acknowledgement after every frame it sends.
- When acknowledgement is received, then only next frame is sent. The process of alternately sending and waiting of a frame continues until the sender transmits the EOT (End of transmission) frame.

Advantage of Stop-and-wait

The Stop-and-wait method is simple as each frame is checked and acknowledged before the next frame is sent.

Disadvantage of Stop-and-wait

Stop-and-wait technique is inefficient to use as each frame must travel across all the way to the receiver and an acknowledgement travels all the way before the next frame is sent. Each frame sent and received uses the entire time needed to traverse the link.

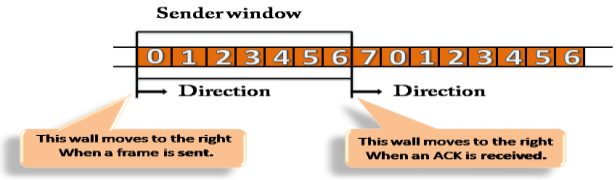
Sliding Window

- The Sliding Window is a method of flow control in which a sender can transmit the several frames before getting an acknowledgement.
- In Sliding Window Control, multiple frames can be sent one after the another due to which capacity of the communication channel can be utilized efficiently.
- A single ACK acknowledge multiple frames.
- Sliding Window refers to imaginary boxes at both the sender and receiver end.
- The window can hold the frames at either end, and it provides the upper limit on the number of frames that can be transmitted before the acknowledgement.
- Frames can be acknowledged even when the window is not completely filled.
- The window has a specific size in which they are numbered as modulo-n means that they are numbered from 0 to n-1. For example, if n = 8, the frames are numbered from 0,1,2,3,4,5,6,7,0,1,2,3,4,5,6,7,0,1.....
- The size of the window is represented as n-1. Therefore, maximum n-1 frames can be sent before acknowledgement.
- When the receiver sends the ACK, it includes the number of the next frame that it wants to receive. For example, to acknowledge the string of frames ending with frame number 4, the receiver will send the ACK containing the number 5. When the sender sees the ACK with the number 5, it got to know that the frames from 0 through 4 have been received.

Sender Window

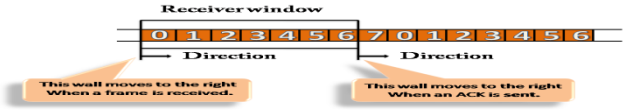
- At the beginning of a transmission, the sender window contains n-1 frames, and when they are sent out, the left boundary moves inward shrinking the size of the window. For example, if the size of the window is w if three frames are sent out, then the number of frames left out in the sender window is w-3.
- Once the ACK has arrived, then the sender window expands to the number which will be equal to the number of frames acknowledged by ACK.
- For example, the size of the window is 7, and if frames 0 through 4 have been sent out and no acknowledgement has arrived, then the sender window contains only two frames, i.e., 5 and 6. Now, if ACK has arrived with a number 4 which means that 0 through 3 frames have arrived undamaged and the sender window is expanded to

include the next four frames. Therefore, the sender window contains six frames (5,6,7,0,1,2).



Receiver Window

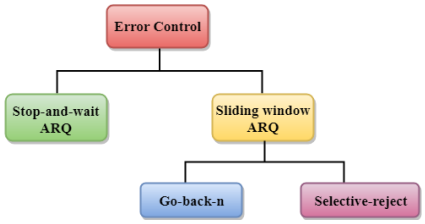
- At the beginning of transmission, the receiver window does not contain n frames, but it contains n-1 spaces for frames.
- When the new frame arrives, the size of the window shrinks.
- The receiver window does not represent the number of frames received, but it represents the number of frames that can be received before an ACK is sent. For example, the size of the window is w, if three frames are received then the number of spaces available in the window is (w-3).
- Once the acknowledgement is sent, the receiver window expands by the number equal to the number of frames acknowledged.
- Suppose the size of the window is 7 means that the receiver window contains seven spaces for seven frames. If the one frame is received, then the receiver window shrinks and moving the boundary from 0 to 1. In this way, window shrinks one by one, so window now contains the six spaces. If frames from 0 through 4 have sent, then the window contains two spaces before an acknowledgement is sent.



Error Control

Error Control is a technique of error detection and retransmission.

Categories of Error Control:



Stop-and-wait ARQ

Stop-and-wait ARQ is a technique used to retransmit the data in case of damaged or lost frames.

This technique works on the principle that the sender will not transmit the next frame until it receives the acknowledgement of the last transmitted frame.

Four features are required for the retransmission:

- The sending device keeps a copy of the last transmitted frame until the acknowledgement is received. Keeping the copy allows the sender to retransmit the data if the frame is not received correctly.
- Both the data frames and the ACK frames are numbered alternately 0 and 1 so that they can be identified individually. Suppose data 1 frame acknowledges the data 0 frames means that the data 0 frames has been arrived correctly and expects to receive data 1 frame.
- If an error occurs in the last transmitted frame, then the receiver sends the NAK frame which is not numbered. On receiving the NAK frame, sender retransmits the data.
- It works with the timer. If the acknowledgement is not received within the allotted time, then the sender assumes that the frame is lost during the transmission, so it will retransmit the frame.

Two possibilities of the retransmission:

- **Damaged Frame:** When the receiver receives a damaged frame, i.e., the frame contains an error, then it returns the NAK frame. For example, when the data 0 frame is sent, and then the receiver sends the ACK 1 frame means that the data 0 has arrived correctly, and transmits the data 1 frame. The sender transmits the next frame: data 1. It reaches undamaged, and the receiver returns ACK 0. The sender transmits the next frame: data 0. The receiver reports an error and returns the NAK frame. The sender retransmits the data 0 frame.
- **Lost Frame:** Sender is equipped with the timer and starts when the frame is transmitted. Sometimes the frame has not arrived at the receiving end so that it can be acknowledged neither positively nor negatively. The sender waits for acknowledgement until the timer goes off. If the timer goes off, it retransmits the last transmitted frame.

Sliding Window ARQ

Sliding Window ARQ is a technique used for continuous transmission error control.

Three Features used for retransmission:

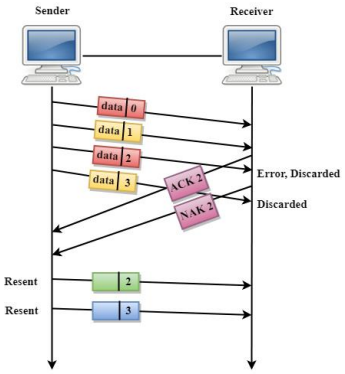
- In this case, the sender keeps the copies of all the transmitted frames until they have been acknowledged. Suppose the frames from 0 through 4 have been transmitted, and the last acknowledgement was for frame 2, the sender has to keep the copies of frames 3 and 4 until they receive correctly.
- The receiver can send either NAK or ACK depending on the conditions. The NAK frame tells the sender that the data have been received damaged. Since the sliding window is a continuous transmission mechanism, both ACK and NAK must be numbered for the identification of a frame. The ACK frame consists of a number that represents the next frame which the receiver expects to receive. The NAK frame consists of a number that represents the damaged frame.
- The sliding window ARQ is equipped with the timer to handle the lost acknowledgements. Suppose then n-1 frames have been sent before receiving any acknowledgement. The sender waits for the acknowledgement, so it starts the timer and waits before sending any more. If the allotted time runs out, the sender retransmits one or all the frames depending upon the protocol used.

Two protocols used in sliding window ARQ:

- **Go-Back-n ARQ:** In Go-Back-N ARQ protocol, if one frame is lost or damaged, then it retransmits all the frames after which it does not receive the positive ACK.

Three possibilities can occur for retransmission:

- **Damaged Frame:** When the frame is damaged, then the receiver sends a NAK frame.

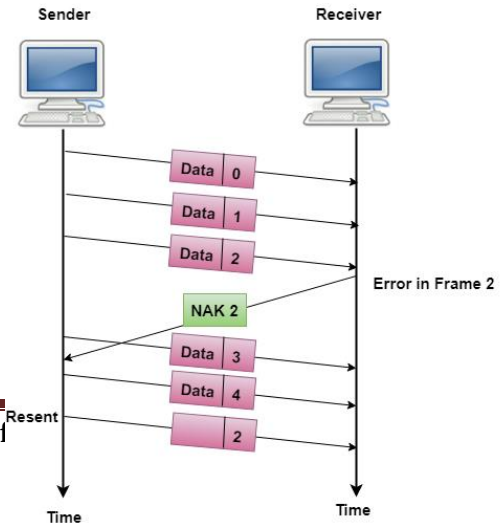


In the above figure, three frames have been transmitted before an error discovered in the third frame. In this case, ACK 2 has been returned telling that the frames 0,1 have been received successfully without any error. The receiver discovers the error in data 2 frame, so it returns the NAK 2 frame. The frame 3 is also discarded as it is transmitted after the damaged frame. Therefore, the sender retransmits the frames 2,3.

- **Lost Data Frame:** In Sliding window protocols, data frames are sent sequentially. If any of the frames is lost, then the next frame arrive at the receiver is out of sequence. The receiver checks the sequence number of each of the frame, discovers the frame that has been skipped, and returns the NAK for the missing frame. The sending device retransmits the frame indicated by NAK as well as the frames transmitted after the lost frame.
- **Lost Acknowledgement:** The sender can send as many frames as the windows allow before waiting for any acknowledgement. Once the limit of the window is reached, the sender has no more frames to send; it must wait for the acknowledgement. If the acknowledgement is lost, then the sender could wait forever. To avoid such situation, the sender is equipped with the timer that starts counting whenever the window capacity is reached. If the acknowledgement has not been received within the time limit, then the sender retransmits the frame since the last ACK.

Selective-Reject ARQ

- Selective-Reject ARQ technique is more efficient than Go-Back-n ARQ.
- In this technique, only those frames are retransmitted for which negative acknowledgement (NAK) has been received.
- The receiver storage buffer keeps all the damaged frames on hold until the frame in error is correctly received.
- The receiver must have an appropriate logic for reinserting the frames in a correct order.
- The sender must consist of a searching mechanism that selects only the requested frame for retransmission.



Data Link Protocols

A protocol in data communication is the set of specifications used to implement one or more layers of the OSI model.

Data link protocols are sets of specifications used to implement the info data link layer to this end, they contain rules for line discipline, flow control, and error handling, among others.

Data link protocols can be divided into two subgroups:-

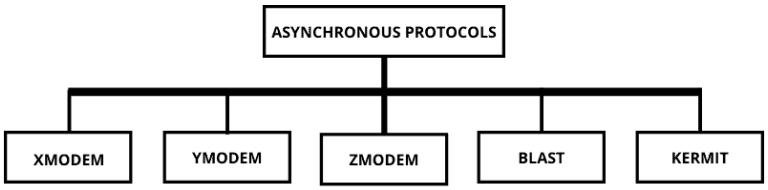
- **Asynchronous protocols**
- **Synchronous protocols.**

Asynchronous protocols treat each character during a bit stream independently. Synchronous protocols take the entire bit stream and chop it into characters of equal size.

Asynchronous Protocols

Many synchronous data link protocols have been developed over the last several decades, one of which is these protocols are employed mainly in modems.

Due to its inherent slowness stemming from the required additions of start and stop bits and extended space between frames, asynchronous transmission at this level is being replaced by higher speed synchronous mechanisms.



Asynchronous protocols aren't complex and are inexpensive to implement. Asynchronous transmission a data unit is transmitted with no timing coordination between the sender and receiver.

A receiver doesn't get to know exactly when a knowledge unit is shipped it only must recognize the beginning and the end of the unit. This is accomplished by using extra bits start and stop bits to frame into the data unit.

There are 5 types of Asynchronous protocols in Datalink protocols, full information about this is given below:-

- **XMODEM**
- **YMODEM**
- **ZMODEM**
- **BLAST**
- **KERMIT**

XMODEM:-

XMODEM in Data link protocols, in 1979 ward Christiansen designed a file transfer protocol for telephonic-line communication between PCs. This protocol, now known as XMODEM, may be a half-duplex stop-and-wait ARQ protocol.

The first field is a one-byte start of the header (SHO). The second field is a two-byte header. The first header byte, the sequence number, carries the frame number.

The second harder byte is used to check the validity of the sequence number. The fixed data field holds 128 bytes of data (binary, ASCII, Boolean, text, etc.). The last field, CRC, checks for errors within the data field only.

In this protocol, transmission begins with the sending of a NAK frame from the receiver to the sender. Each time the sender sends a frame, it waits for an acknowledgment (ACK) before the next frame can be sent. If instead of a NAK is received, the previously sent frame is sent again.

A frame can also be resent i\if a response is not received by the sender after a specified amount of time. Besides a NAK or an ACK, the sender can receive a cancel single (CAN), which aborts the transmission.

YMODEM:-

YMODEM is a type of Data link protocol that is similar to XMODEM, with the subsequent major differences:

- The data unit is 1024 bytes.
- Two CANs are sent to abort a transmission.
- ITU-T CRC-16 is used for error checking.
- Multiple files can be sent simultaneously.

ZMODEM:-

Modems a newer protocol combining features of both XMODEM and YMODEM.

BLAST:-

Blocked asynchronous transmission (BLAST) is more powerful than XMODEM. It is a full-duplex with sliding window flow control. It allows the transmission of data and binary files.

KERMIT:-

KERMIT is another type of data link protocol, which is designed at Columbia University, is currently the foremost widely used asynchronous protocol.

This file transfer protocol is similar in operation to XMODEM, with the sender waiting for a NAK before it starts transmission. Kermit allows the transmission of control characters as text using two steps.

First, the control character, which is used as text, is transformed into a printable character by adding a fixed number to its ASCII code representation.

Second, the # character is added to the front of the transformed character.

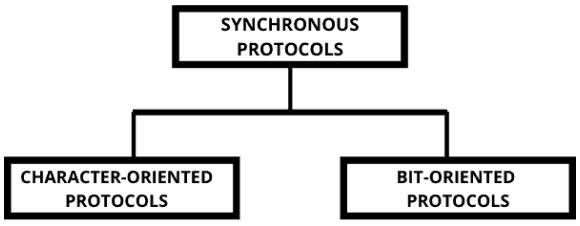
In this way, a control character is used as the text is sent as two characters. When the receiver encounters a # character, it knows that this must be dropped which the next character is a control character. If the sender wants to send a # character, it'll send two of them.

Synchronous Protocols

Now you are going to learn about synchronous protocols in data link protocols, and about their types.

The speed of synchronous transmission makes it the better choice, over the synchronous transmission, For LAN, MAN, and WAN technology. Protocols governing synchronous transmission are often divided into two classes:

- **character-oriented protocols**
- **bit-oriented protocols**



Character-Oriented Protocols:-

Character-oriented protocols (also called byte-oriented protocols) interpret a transmission frame or packet as a succession of characters, each usually composed of one byte (eight bits). All control information is within sort of an existing character encoding system.

Bit-Oriented Protocols:-

Bit-oriented protocols interpret a transfer frame or packet as a succession of individual bits, made meaningful by their placement in the frame and by their juxtaposition with other bits. Control information during a bit-oriented protocol is often one or multiple bits depending on the information embodied in the pattern.

If you found this helpful about data link protocols then please comment, and give your valuable suggestion to make your experience better.

Multiple access protocol- ALOHA, CSMA, CSMA/CA and CSMA/CD

Data Link Layer

The data link layer is used in a computer network to transmit the data between two devices or nodes. It divides the layer into parts such as **data link control** and the **multiple access resolution/protocol**. The upper layer has the responsibility to flow control and the error control in the data link layer, and hence it is termed as **logical of data link control**. Whereas the lower sub-layer is used to handle and reduce the collision or multiple access on a channel. Hence it is termed as media access control or the multiple access resolutions.

Data Link Control

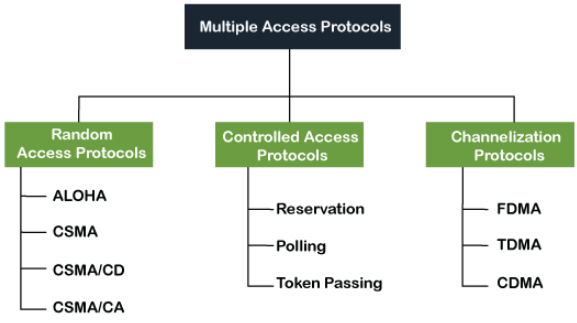
A data link control is a reliable channel for transmitting data over a dedicated link using various techniques such as framing, error control and flow control of data packets in the computer network.

What is a multiple access protocol?

When a sender and receiver have a dedicated link to transmit data packets, the data link control is enough to handle the channel. Suppose there is no dedicated path to communicate or transfer the data between two devices. In that case, multiple stations access the channel and simultaneously transmit the data over the channel. It may create collision and cross talk. Hence, the multiple access protocol is required to reduce the collision and avoid crosstalk between the channels.

For example, suppose that there is a classroom full of students. When a teacher asks a question, all the students (small channels) in the class start answering the question at the same time (transferring the data simultaneously). All the students respond at the same time due to which data is overlap or data lost. Therefore it is the responsibility of a teacher (multiple access protocol) to manage the students and make them one answer.

Following are the types of multiple access protocol that is subdivided into the different process as:



A. Random Access Protocol

In this protocol, all the station has the equal priority to send the data over a channel. In random access protocol, one or more stations cannot depend on another station nor any station control another station. Depending on the channel's state (idle or busy), each station transmits the data frame. However, if more than one station sends the data over a channel, there may be a collision or data conflict. Due to the collision, the data frame packets may be lost or changed. And hence, it does not receive by the receiver end.

Following are the different methods of random-access protocols for broadcasting frames on the channel.

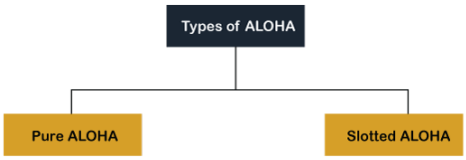
- Aloha
- CSMA
- CSMA/CD
- CSMA/CA

ALOHA Random Access Protocol

It is designed for wireless LAN (Local Area Network) but can also be used in a shared medium to transmit data. Using this method, any station can transmit data across a network simultaneously when a data frameset is available for transmission.

Aloha Rules

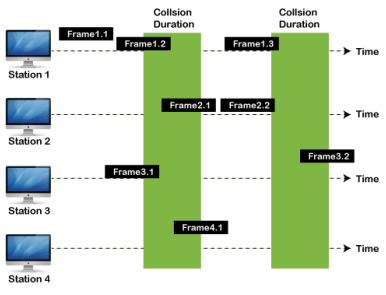
1. Any station can transmit data to a channel at any time.
2. It does not require any carrier sensing.
3. Collision and data frames may be lost during the transmission of data through multiple stations.
4. Acknowledgment of the frames exists in Aloha. Hence, there is no collision detection.
5. It requires retransmission of data after some random amount of time.



Pure Aloha

Whenever data is available for sending over a channel at stations, we use Pure Aloha. In pure Aloha, when each station transmits data to a channel without checking whether the channel is idle or not, the chances of collision may occur, and the data frame can be lost. When any station transmits the data frame to a channel, the pure Aloha waits for the receiver's acknowledgment. If it does not acknowledge the receiver end within the specified time, the station waits for a random amount of time, called the backoff time (Tb). And the station may assume the frame has been lost or destroyed. Therefore, it retransmits the frame until all the data are successfully transmitted to the receiver.

1. The total vulnerable time of pure Aloha is 2 * Tfr.
2. Maximum throughput occurs when G = 1/ 2 that is 18.4%.
3. Successful transmission of data frame is S = G * e ^ - 2 G.



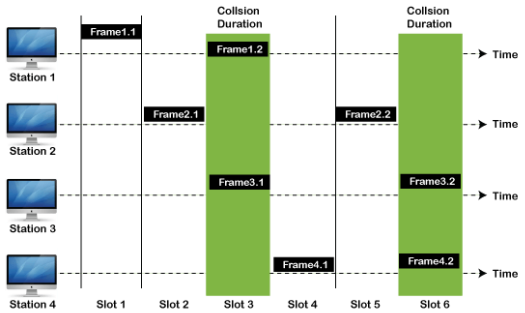
Frames in Pure ALOHA

As we can see in the figure above, there are four stations for accessing a shared channel and transmitting data frames. Some frames collide because most stations send their frames at the same time. Only two frames, frame 1.1 and frame 2.2, are successfully transmitted to the receiver end. At the same time, other frames are lost or destroyed. Whenever two frames fall on a shared channel simultaneously, collisions can occur, and both will suffer damage. If the new frame's first bit enters the channel before finishing the last bit of the second frame. Both frames are completely finished, and both stations must retransmit the data frame.

Slotted Aloha

The slotted Aloha is designed to overcome the pure Aloha's efficiency because pure Aloha has a very high possibility of frame hitting. In slotted Aloha, the shared channel is divided into a fixed time interval called **slots**. So that, if a station wants to send a frame to a shared channel, the frame can only be sent at the beginning of the slot, and only one frame is allowed to be sent to each slot. And if the stations are unable to send data to the beginning of the slot, the station will have to wait until the beginning of the slot for the next time. However, the possibility of a collision remains when trying to send a frame at the beginning of two or more station time slot.

1. Maximum throughput occurs in the slotted Aloha when G = 1 that is 37%.
2. The probability of successfully transmitting the data frame in the slotted Aloha is S = G * e ^ - 2 G.
3. The total vulnerable time required in slotted Aloha is Tfr.



Frames in Slotted ALOHA

CSMA (Carrier Sense Multiple Access)

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.

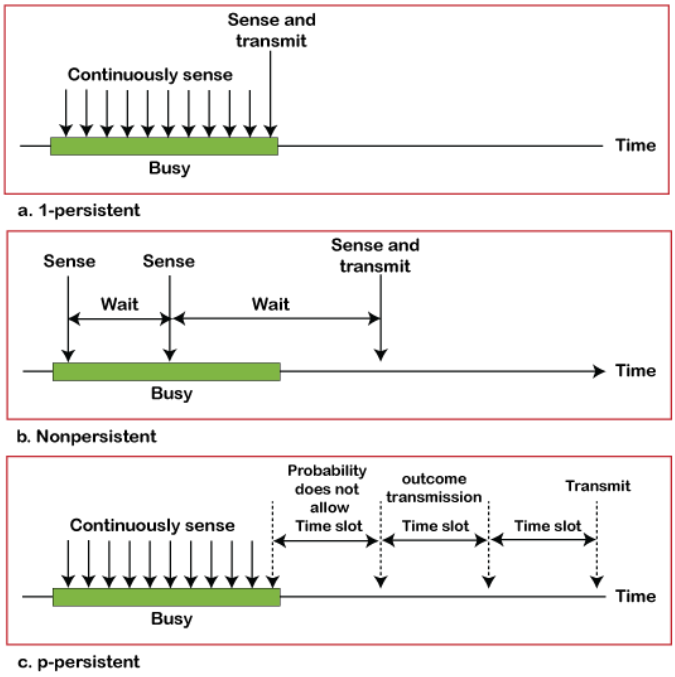
CSMA Access Modes

1-Persistent: In the 1-Persistent mode of CSMA that defines each node, first sense the shared channel and if the channel is idle, it immediately sends the data. Else it must wait and keep track of the status of the channel to be idle and broadcast the frame unconditionally as soon as the channel is idle.

Non-Persistent: It is the access mode of CSMA that defines before transmitting the data, each node must sense the channel, and if the channel is inactive, it immediately sends the data. Otherwise, the station must wait for a random time (not continuously), and when the channel is found to be idle, it transmits the frames.

P-Persistent: It is the combination of 1-Persistent and Non-persistent modes. The P-Persistent mode defines that each node senses the channel, and if the channel is inactive, it sends a frame with a **P** probability. If the data is not transmitted, it waits for a (**q = 1-p probability**) random time and resumes the frame with the next time slot.

O- Persistent: It is an O-persistent method that defines the superiority of the station before the transmission of the frame on the shared channel. If it is found that the channel is inactive, each station waits for its turn to retransmit the data.



CSMA/ CD

It is a **carrier sense multiple access/ collision detection** network protocol to transmit data frames. The CSMA/CD protocol works with a medium access control layer. Therefore, it first senses the shared channel before broadcasting the frames, and if the channel is idle, it transmits a frame to check whether the transmission was successful. If the frame is successfully received, the station sends another frame. If any collision is detected in the CSMA/CD, the station sends a jam/ stop signal to the shared channel to terminate data transmission. After that, it waits for a random time before sending a frame to a channel.

CSMA/ CA

It is a **carrier sense multiple access/collision avoidance** network protocol for carrier transmission of data frames. It is a protocol that works with a medium access control layer. When a data frame is sent to a channel, it receives an acknowledgment to check whether the channel is clear. If the station receives only a single (own) acknowledgments, that means the data frame has been successfully transmitted to the receiver. But if it gets two signals (its own and one more in which the collision of frames), a collision of the frame occurs in the shared channel. Detects the collision of the frame when a sender receives an acknowledgment signal. Following are the methods used in the CSMA/ CA to avoid the collision:

Interframe space: In this method, the station waits for the channel to become idle, and if it gets the channel is idle, it does not immediately send the data. Instead of this, it waits for some time, and this time period is called the Interframe space or IFS. However, the IFS time is often used to define the priority of the station.

Contention window: In the Contention window, the total time is divided into different slots. When the station/ sender is ready to transmit the data frame, it chooses a random slot number of slots as wait time. If the channel is still busy, it does not restart the entire process, except that it restarts the timer only to send data packets when the channel is inactive.

Acknowledgment: In the acknowledgment method, the sender station sends the data frame to the shared channel if the acknowledgment is not received ahead of time.

B. Controlled Access Protocol

It is a method of reducing data frame collision on a shared channel. In the controlled access method, each station interacts and decides to send a data frame by a particular station approved by all other stations. It means that a single station cannot send the data frames unless all other stations are not approved. It has three types of controlled access: **Reservation, Polling**, and **Token Passing**.

C. Channelization Protocols

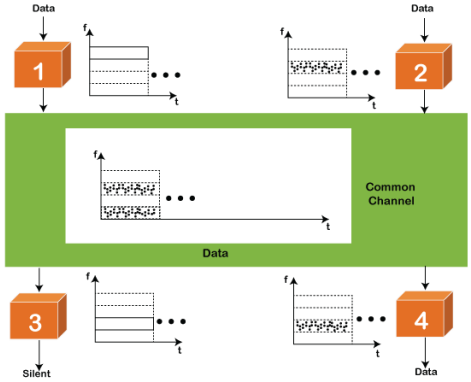
It is a channelization protocol that allows the total usable bandwidth in a shared channel to be shared across multiple stations based on their time, distance and codes. It can access all the stations at the same time to send the data frames to the channel.

Following are the various methods to access the channel based on their time, distance and codes:

1. FDMA (Frequency Division Multiple Access)
2. TDMA (Time Division Multiple Access)
3. CDMA (Code Division Multiple Access)

FDMA

It is a frequency division multiple access (**FDMA**) method used to divide the available bandwidth into equal bands so that multiple users can send data through a different frequency to the subchannel. Each station is reserved with a particular band to prevent the crosstalk between the channels and interferences of stations.



TDMA

Time Division Multiple Access (**TDMA**) is a channel access method. It allows the same frequency bandwidth to be shared across multiple stations. And to avoid collisions in the shared channel, it divides the channel into different frequency slots that allocate stations to transmit the data frames. The same **frequency** bandwidth into the shared channel by dividing the signal into various time slots to transmit it. However, TDMA has an overhead of synchronization that specifies each station's time slot by adding synchronization bits to each slot.

CDMA

The code division multiple access (CDMA) is a channel access method. In CDMA, all stations can simultaneously send the data over the same channel. It means that it allows each station to transmit the data frames with full frequency on the shared channel at all times. It does not require the division of bandwidth on a shared channel based on time slots. If multiple stations send data to a channel simultaneously, their data frames are separated by a unique code sequence. Each station has a different unique code for transmitting the data over a shared channel. For example, there are multiple users in a room that are continuously speaking. Data is received by the users if only two-person interact with each other using the

same language. Similarly, in the network, if different stations communicate with each other simultaneously with different code language.

PPP Protocol

The PPP stands for Point-to-Point protocol. It is the most commonly used protocol for point-to-point access. Suppose the user wants to access the internet from the home, the PPP protocol will be used.

It is a data link layer protocol that resides in the layer 2 of the OSI model . It is used to encapsulate the layer 3 protocols and all the information available in the payload in order to be transmitted across the serial links. The PPP protocol can be used on synchronous link like ISDN as well as asynchronous link like dial-up. It is mainly used for the communication between the two devices.

It can be used over many types of physical networks such as serial cable, phone line, trunk line, cellular telephone, fiber optic links such as SONET. As the data link layer protocol is used to identify from where the transmission starts and ends, so ISP (Internet Service Provider) use the PPP protocol to provide the dial-up access to the internet.

Services provided by PPP

- It defines the format of frames through which the transmission occurs.
- It defines the link establishment process. If user establishes a link with a server, then "how this link establishes" is done by the PPP protocol.
- It defines data exchange process, i.e., how data will be exchanged, the rate of the exchange.
- The main feature of the PPP protocol is the encapsulation. It defines how network layer data and information in the payload are encapsulated in the data link frame.
- It defines the authentication process between the two devices. The authentication between the two devices, handshaking and how the password will be exchanged between two devices are decided by the PPP protocol.

Services not provided by the PPP protocol

- It does not support flow control mechanism.
- It has a very simple error control mechanism.
- As PPP provides point-to-point communication, so it lacks addressing mechanism to handle frames in multipoint configuration.

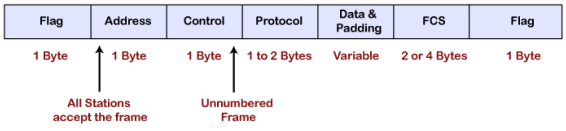
It is a byte-oriented protocol as it provides the frames as a collection of bytes or characters. It is a WAN (Wide Area Network) protocol as it runs over the internet link which means between two routers, internet is widely used.

PPP has two main uses which are given below:

- It is widely used in broadband communications having heavy loads and high speed. For example, an internet operates on heavy load and high speed.
- It is used to transmit the multiprotocol data between the two connected (point-to-point) computers. It is mainly used in point-to-point devices, for example, routers are point-to-point devices where PPP protocol is widely used as it is a WAN protocol not a simple LAN ethernet protocol.

Frame format of PPP protocol

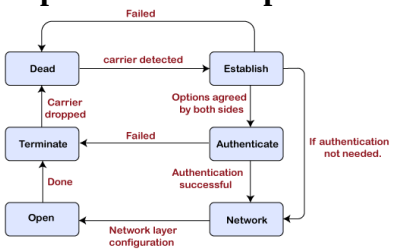
The frame format of PPP protocol contains the following fields:



- **Flag:** The flag field is used to indicate the start and end of the frame. The flag field is a 1-byte field that appears at the beginning and the ending of the frame. The pattern of the flag is similar to the bit pattern in HDLC, i.e., 01111110.
- **Address:** It is a 1-byte field that contains the constant value which is 11111111. These 8 ones represent a broadcast message.
- **Control:** It is a 1-byte field which is set through the constant value, i.e., 11000000. It is not a required field as PPP does not support the flow control and a very limited error control mechanism. The control field is a mandatory field where protocol supports flow and error control mechanism.
- **Protocol:** It is a 1 or 2 bytes field that defines what is to be carried in the data field. The data can be a user data or other information.
- **Payload:** The payload field carries either user data or other information. The maximum length of the payload field is 1500 bytes.
- **Checksum:** It is a 16-bit field which is generally used for error detection.

Transition phases of PPP protocol

The following are the transition phases of a PPP protocol:



Transition phases

- **Dead:** Dead is a transition phase which means that the link is not used or there is no active carrier at the physical layer.
- **Establish:** If one of the nodes starts working then the phase goes to the establish phase. In short, we can say that when the node starts communication or carrier is detected then it moves from the dead to the establish phase.
- **Authenticate:** It is an optional phase which means that the communication can also moves to the authenticate phase. The phase moves from the establish to the authenticate phase only when both the communicating nodes agree to make the communication authenticated.
- **Network:** Once the authentication is successful, the network is established or phase is network. In this phase, the negotiation of network layer protocols take place.
- **Open:** After the establishment of the network phase, it moves to the open phase. Here open phase means that the exchange of data takes place. Or we can say that it reaches to the open phase after the configuration of the network layer.
- **Terminate:** When all the work is done then the connection gets terminated, and it moves to the terminate phase.

On reaching the terminate phase, the link moves to the dead phase which indicates that the carrier is dropped which was earlier created.

There are two more possibilities that can exist in the transition phase:

- The link moves from the authenticate to the terminate phase when the authentication is failed.
- The link can also move from the establish to the dead state when the carrier is failed.

PPP Stack

In PPP stack, there are three set of protocols:

- **Link Control Protocol (LCP)**

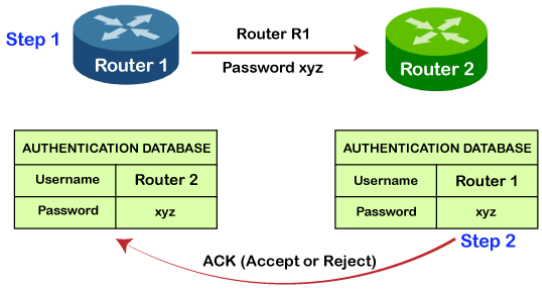
The role of LCP is to establish, maintain, configure, and terminate the links. It also provides negotiation mechanism.

- **Authentication protocols**

There are two types of authentication protocols, i.e., PAP (Password Authenticate protocols), and CHAP (Challenged Handshake Authentication Protocols).

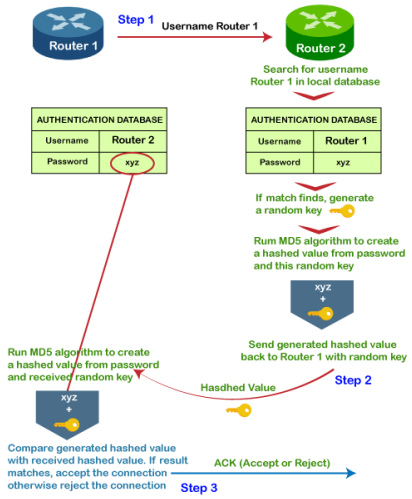
1. PAP (Password Authentication Protocols)

PAP is less secure as compared to CHAP as in case of PAP protocol, password is sent in the form of a clear text. It is a two-step process. Suppose there are two routers, i.e., router 1 and router 2. In the first step, the router 1 wants to authenticate so it sends the username and password for the authentication. In the second step, if the username and password are matched then the router 2 will authenticate the router 1 otherwise the authentication failed.



2. CHAP (Challenged Handshake Authentication Protocol)

CHAP is a three-step process. Let's understand the three steps of CHAP.



Step 1: Suppose there are two routers, i.e., router 1 and router 2. In this step, router 1 sends the username but not the password to the router 2.

Step 2: The router 2 maintains a database that contains a list of allowed hosts with their login credentials. If no data is found which means that the router 1 is not a valid host to connect with it and the connection gets terminated. If the match is found then the random key is passed. This random key along with the password is passed in the MD5 hashing function, and the hashing function generates the hashed value from the password and the random key (password + random key). The hashed value is also known as Challenge. The challenge along with the random key will be sent to the router 1.

Step 3: The router 1 receives the hashed value and a random key from the router 2. Then, the router 1 will pass the random key and locally stored password to the MD5 hashing function. The MD5 hashing function generates the hashed value from the combination of random key and password. If the generated hashed value does not match with the received hashed value then the connection gets terminated. If it is matched, then the connection is granted. Based on

the above authentication result, the authentication signal that could be either accepted or rejected is sent to the router 2.

- **Network Control Protocol (NCP)**

After the establishment of the link and authentication, the next step is to connect to the network layer. So, PPP uses another protocol known as network control protocol (NCP). The NCP is a set of protocols that facilitates the encapsulation of data which is coming from the network layer to the PPP frames.

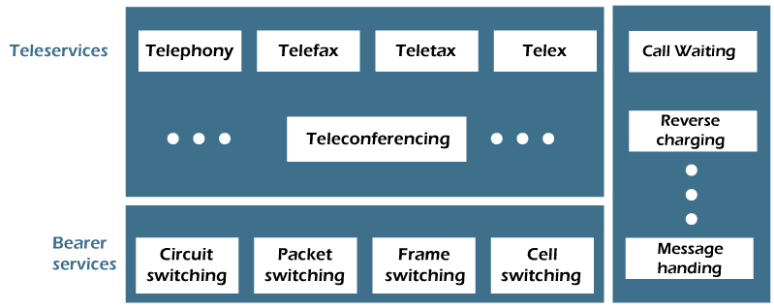
Integrated Services Digital Network

In this article will learn about the ISDN. In this we will learn about the introduction, various principle, services and ISDN channels in detail.

Introduction:

ISDN is a set of protocols that is based on high-speed fully digitized telephone service. The main aim of ISDN is to provide a fully integrated digital service to the users.

In ISDN there are following three types of ISDN services:



Bearer Services:

This type of services is used to transfer information such as voice, data, and video between the users without manipulating the content of the network information. It belongs to the first 3 layers of the OSI reference model.

Tele Services:

In these types of services, the network may change the contents of the data. It belongs to the last 4 layers of the OSI reference model. It includes telephony, tele box, fax, and teleconferencing etc.

Supplementary Services:

It provides additional functionality to the bearer services and teleservices. Some of the examples of supplementary services are reverse charging, call waiting, and message handling.

Principles of ISDN:

Following are the principles of ISDN are:

- It supports both circuit switching & packet switching with the connections at 64 kbps.
- In ISDN layered protocol architecture is used for specification.
- ISDN services provides maintenance.
- ISDN services includes some network management functions.
- In ISDN network several configurations are possible for implementing.

ISDN SERVICES:

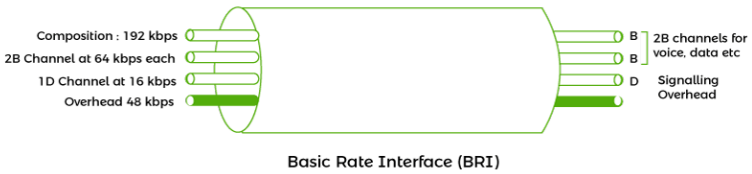
Following are the two types of services associated with ISDN:

Basic Rate Interface:

In the Basic Rate Interface digital pipe consists of 2 B channels and a 1 D channel. Therefore it is denoted as "2B + 1 D". These two B channels have a data rate of 64 kbps each, and the D channel have a data rate of 16 kbps. It has also a usable bandwidth of 144 kbps.

Basic Rate Interface allows the concurrent use of voice and various data applications such as packet-switched access, a link to a central alarm service, video, tax, etc. The signaling information for the two channels is sent onto the D channel. The two B channels can be used for one 128 kbps connection or two independent connections on the two channels.

The following figure shows the basic structure of the frame in the Basic Rate Interface is:



Basic Rate Interface (BRI)

This service is used to meet the needs of most individual users, including residential and small offices. In this case, the two B channels and the D channel are multiplexed with overhead bits in the form of the frame structure. The overhead bits include framing, DC balancing, and other bits.

The 48 bit frame consists of

- 16 bits of B1 Channel
- 16 bits of B2 Channel
- 4 bits of D channel
- 12 overhead bits

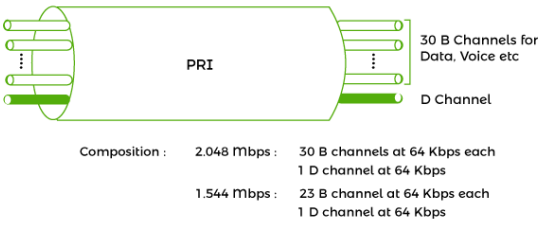
The frame is transmitted in 250 µsec, which results in the following bit rates:

- In frame each B channel = 16 / 250 µsec = 64 kbps
- In frame D channel = 4 / 250 µsec = 16 kbps
- In frame Overhead Bits = 12 / 250 µsec = 48 kbps
- In frame Overall Bit rate = 48 / 250 µsec = 192 kbps

Primary Rate Interface:

Primary Rate Interface consists of either 23 B channels or 30 B channels and a one 64 Kbps D channel. In North America and the Japan, 23 B channels and one D channel are used. It is also denoted by '23 B + 1 D'. In addition, the Primary Rate Interface service itself uses 8 kbps of overhead. Therefore 23D + 1D requires a data rate of 1.544 Mbps. In the case of 30 B channels and one D channel, the total bit rate is 2.048 Mbps.

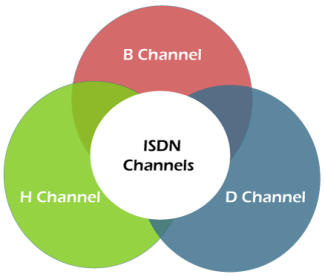
The following figure shows the basic structure of the frame in the Primary Rate Interface is:



ISDN CHANNELS:

ISDN structure have a central ISDN office in which all the users are linked to this through a digital pipe. This digital pipe have different capacities and have a different data transfer rates and these are organized into multiple channels of different sizes.

ISDN standard have the following three types of channels:



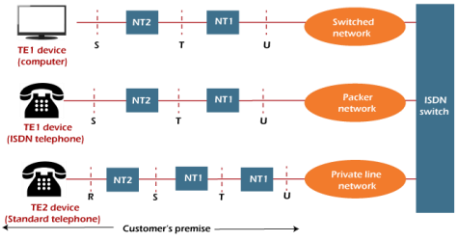
B Channel:
It stands for Bearer channel. It has a 64 kbps standard data rate. It is a basic user channel and can carry any digital information in full-duplex mode. In this transmission rate does not exceed 64 kbps. It can carry digital voice, digital data, and any other low data rate information.

D Channel:
It stands for Data Channel. This channel carry control signal for bearer services. This channel is required for signaling or packet-switched data and all-controlling signals such as establishing calls, ringing, call interrupt, etc.

H Channel:
It stands for Hybrid Channel. It provides user information at higher bit rates.
There are 3 types of Hybrid Channel depending on the data rates. Following are the hybrid channels types:

- Hybrid Channel 0 with 384 kbps data rate.
- Hybrid Channel 11 with 1536 kbps data rate.
- Hybrid Channel 12 with 1920 kbps data rate.

ISDN Devices:
Following are the types of ISDN devices:
TE1: Terminal equipment type (TE1) are specialized ISDN terminals. It includes digital telephone instruments such as FAX, or data terminal equipment. All these devices have an S-bus ISDN interface.
TE2: Terminal equipment type (TE2) is Non-ISDN compatible is connected through a Terminal Adapter. It includes analog phones and 3270 terminal Fax.
TA: It stands for Terminal Adapter. This device acts as an intermediary device for non-ISDN terminal devices. It converts the non-ISDN interface of these devices to the ISDN interface. The ISDN terminal Adapter can be either a standalone device or a board inside the Terminal equipment type 2. Some of the examples of Terminal adapter are EIA/TIA-232-C, V.24 etc.
NT1: It stands for Network termination type 1. It provides a line termination at the customer's premise. They can also provide line monitoring, power feeding, error statistics, and proper timing.
NT2: It stands for Network termination type 2. It provides a switching, multiplexing, concentrating, or distributing information for the customer's premises. Some examples of Network termination type 2 are this could be a LAN server or Private Branch Exchange etc.
ISDN Reference Points:
It specifies the number of reference points that provide interfaces between the adjacent devices.
Following Figure displays the working of ISDN reference points:



In the above figure it shows an ISDN configuration in which 3 devices attached to an ISDN switch at the central office. In which 2 devices are ISDN compatible and they are attached through the S reference point to Network termination type 2 devices. Out of these third device is a standard non-ISDN telephone and is attached to a Terminal Adapter through an R reference point.

These reference points are R, S, T, and U.

- **R:** It stands for Rate transfer point. It is an interface for non-ISDN devices and therefore is the reference point between non-ISDN equipment and a Terminal Adapter. It can be RS-232-C, V, or X series of ITU-T standard or ordinary telephone interface with two wires.
- **S:** It stands for System transfer point. The interface between the user terminal and NT2. It is a four-wire balanced to which upto eight ISDN terminals can be connected. The physical connector for S - interface on terminals and NT1 is an 8-pin RJ-45 connector.
- **T:** It stands for Terminal transfer point. It is the interface between Network termination type 1 and Network termination type 2
- **U:** It is the interface between Network termination type 1 device and the line termination equipment in the carrier network. The U interface is the local copper pair of the access network. The same pair is used for full-duplex transmission of digital signals.