UNIT – III

Apply briefly about error detection with example

Error Detection:

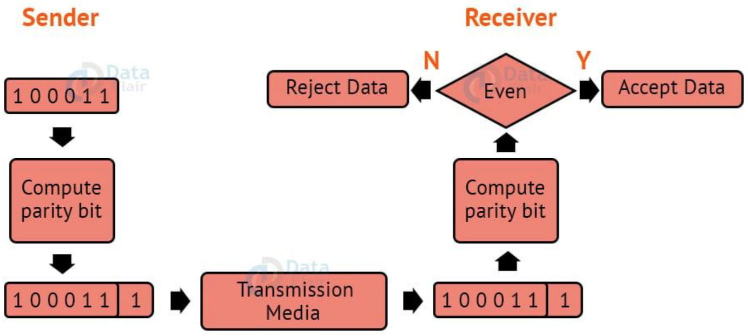
When a message is sent, it may be jumbled by noise or the data may be damaged. To avoid this, we employ error-detecting codes, which are bits of extra data appended to a digital message to assist us detect whether an error occurred during transmission.

Error Detection Techniques:

1. Simple Parity Check:

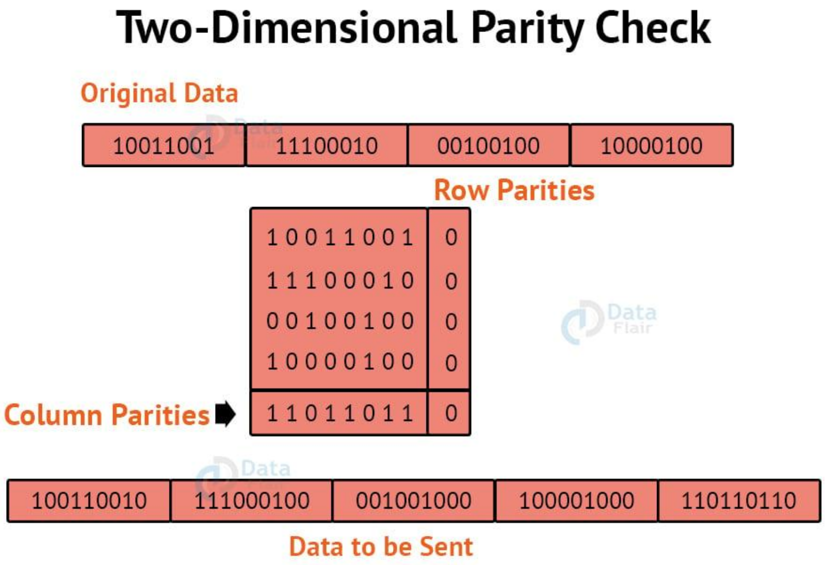
- One extra bit is transmitted in addition to the original bits to make the number of 1s even in the case of even parity or odd in the case of odd parity.
- While creating a frame, the sender counts the amount of 1s in it. If even parity is utilised and the number of 1s is even, one bit with the value 0 is added. In this manner, the number of 1s remains even. If the number of 1s is odd, a value 1 is added to make it even.
- The receiver just counts how many 1s are in a frame. If the number of 1s is even and even parity is utilised, the frame is regarded as uncorrupted and approved. Even if the number of 1s is odd and odd parity is utilised, the frame is not damaged.

Example of Simple Even Parity Check



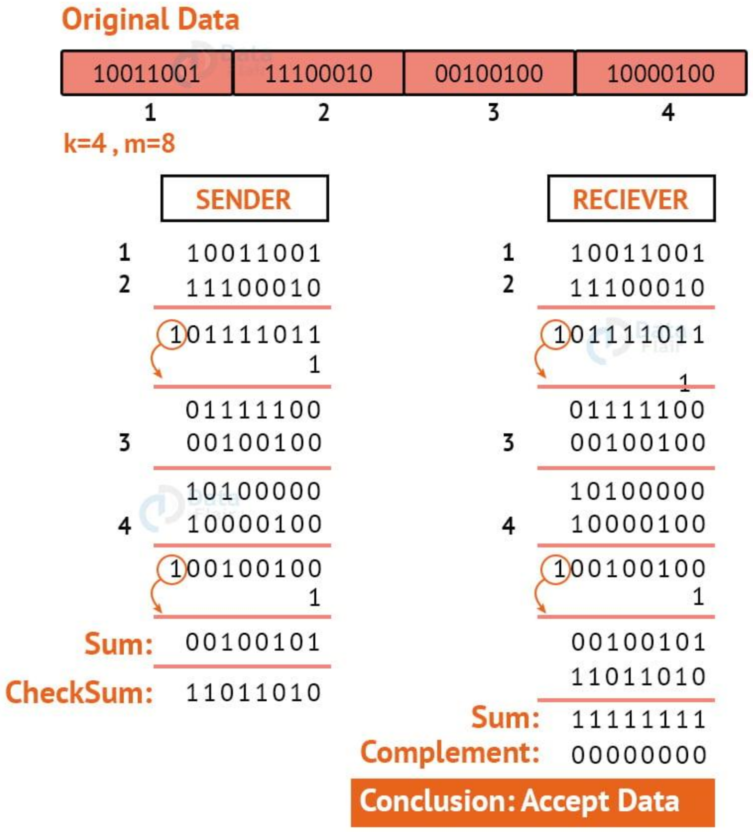
2. Two-Dimensional Parity Check:

For each row, parity check bits are calculated, which is identical to a basic parity check bit. For each column, parity check bits are computed and transmitted together with the data. These are compared with the parity bits calculated on the received data at the receiving end.



3. Checksum:

- The data is split into k segments of m bits each in the checksum error detection technique.
- To get the total, the segments are summed at the sender's end using 1's complement arithmetic. To obtain the checksum, a complement of the sum is taken.
- The checksum segment is sent with the data segments.
- To obtain the total, all received segments are summed using 1's complement arithmetic at the receiver's end. The sum is then calculated.
- If the result is 0, the data is accepted; otherwise, it is rejected.

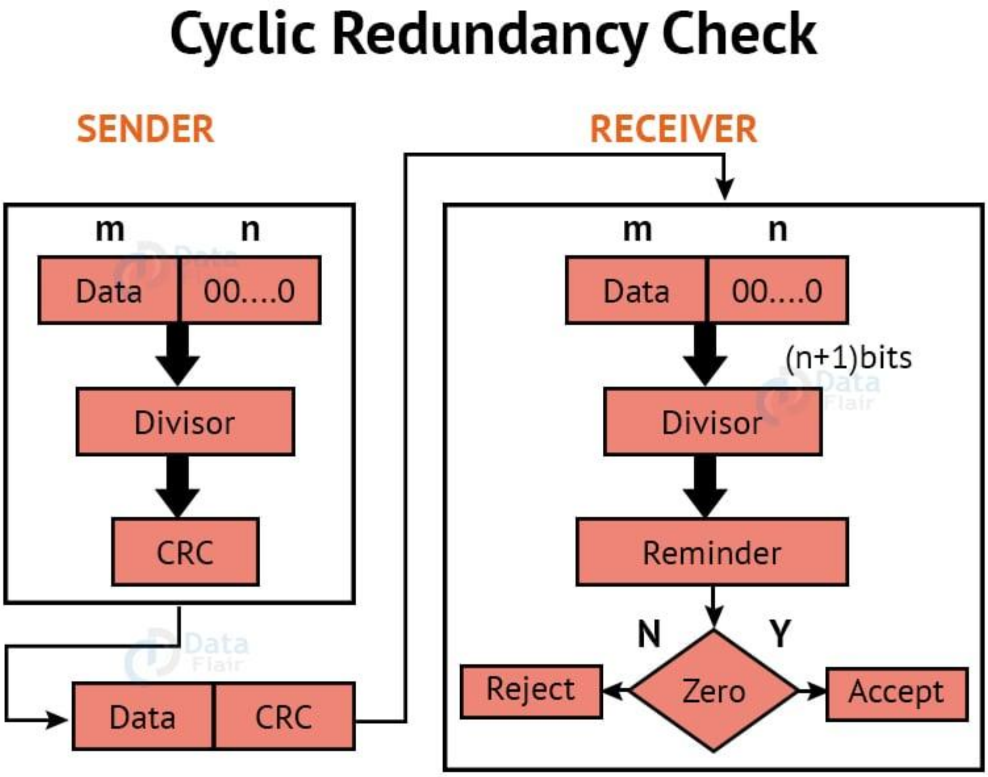


4. Cyclic Redundancy Check:

CRC is an alternative method for determining whether or not a received frame includes valid data. The binary division of the data bits being delivered is used in this approach. Polynomials are used to generate the divisor.

The sender divides the bits that are being transferred and calculates the remainder. The sender inserts the remainder at the end of the original bits before sending the actual bits. A codeword is made up of the actual data bits plus the remainder. The transmitter sends data bits in the form of codewords.

The receiver, on the other hand, divides the codewords using the same CRC divisor. If the remainder consists entirely of zeros, the data bits are validated; otherwise, it is assumed that some data corruption happened during transmission.



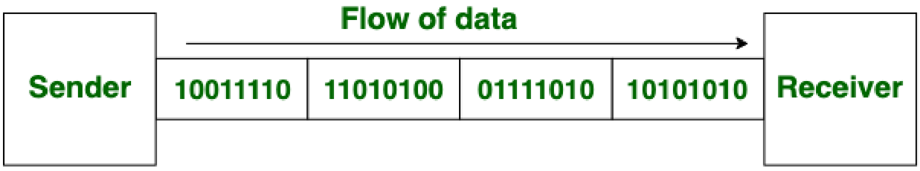
Construct Asynchronous and Synchronous Transmission

Synchronous Transmission:

- In Synchronous Transmission, data is sent in form of blocks or frames. This transmission is the full-duplex type. Between sender and receiver, synchronization is compulsory.
- In Synchronous transmission, There is no gap present between data. It is more efficient and more reliable than asynchronous transmission to transfer a large amount of data.

Example:

- Chat Rooms
- Telephonic Conversations
- Video Conferencing



Synchronous Transmission

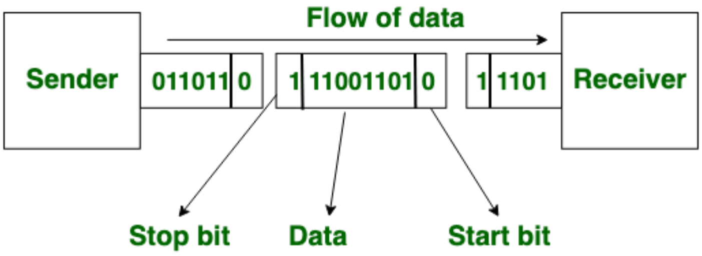
Asynchronous Transmission:

In Asynchronous Transmission, data is sent in form of byte or character. This transmission is the half-duplex type transmission.

In this transmission start bits and stop bits are added with data. It does not require synchronization.

Example:

- Email
- Forums
- Letters



Asynchronous Transmission

S.	Synchronous Transmission	Asynchronous Transmission
1.	In Synchronous transmission, data is sent in form of blocks or frames.	In Asynchronous transmission, data is sent in form of bytes or characters.
2.	Synchronous transmission is fast.	Asynchronous transmission is slow.
3.	Synchronous transmission is costly.	Asynchronous transmission is economical.
4.	In Synchronous transmission, the time interval of transmission is constant.	In Asynchronous transmission, the time interval of transmission is not constant, it is random.
5.	In this transmission, users have to wait till the transmission is complete before getting a response back from the server.	Here, users do not have to wait for the completion of transmission in order to get a response from the server.
6.	In Synchronous transmission, there is no gap present between data.	In Asynchronous transmission, there is a gap present between data.
7.	Efficient use of transmission lines is done in synchronous transmission.	While in Asynchronous transmission, the transmission line remains empty during a gap in character transmission.
8.	The start and stop bits are not used in transmitting data.	The start and stop bits are used in transmitting data that imposes extra overhead.

S.	Synchronous Transmission	Asynchronous Transmission
9.	Synchronous transmission needs precisely synchronized clocks for the information of new bytes.	Asynchronous transmission does not need synchronized clocks as parity bit is used in this transmission for information of new bytes.

Organize an digital data and analog signals

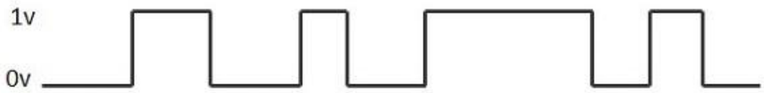
Digital data to Analog signals − The modulation techniques such as

- Amplitude Shift Keying ASK,
- Frequency Shift Keying FSK,
- Phase Shift Keying PSK, etc.,

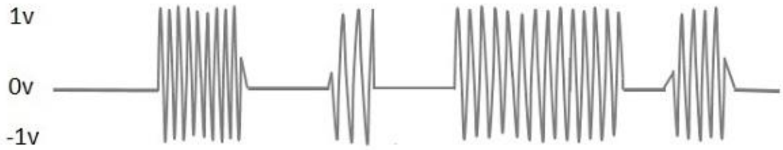
fall under this category. These will be discussed in subsequent chapters

Amplitude Shift Keying

- ASKis a type of Amplitude Modulation which represents the binary data in the form of variations in the amplitude of a signal.
- Any modulated signal has a high frequency carrier. The binary signal when ASK modulated, gives a **zero** value for **Low** input while it gives the **carrier output** for **High** input.
- The following figure represents ASK modulated waveform along with its input.



Input binary sequence

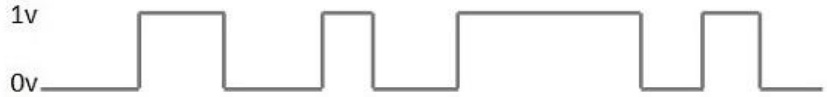


ASK Modulated output wave

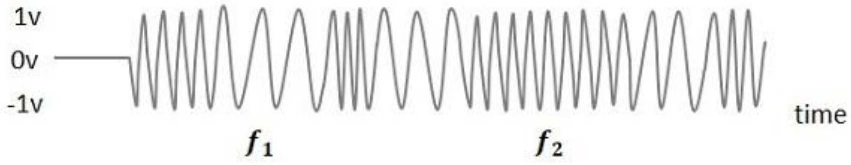
To find the process of obtaining this ASK modulated wave, let us learn about the working of the ASK modulator.

Frequency Shift Keying

- FSK is the digital modulation technique in which the frequency of the carrier signal varies according to the digital signal changes. FSK is a scheme of frequency modulation.
- The output of a FSK modulated wave is high in frequency for a binary High input and is low in frequency for a binary Low input. The binary **1s** and **0s** are called Mark and Space frequencies.
- The following image is the diagrammatic representation of FSK modulated waveform along with its input.



Input binary sequence



FSK Modulated output wave

To find the process of obtaining this FSK modulated wave, let us know about the working of a FSK modulator.

Phase Shift Keying

PSK is the digital modulation technique in which the phase of the carrier signal is changed by varying the sine and cosine inputs at a particular time. PSK technique is widely used for wireless LANs, bio-metric, contactless operations, along with RFID and Bluetooth communications.

PSK is of two types, depending upon the phases the signal gets shifted. They are

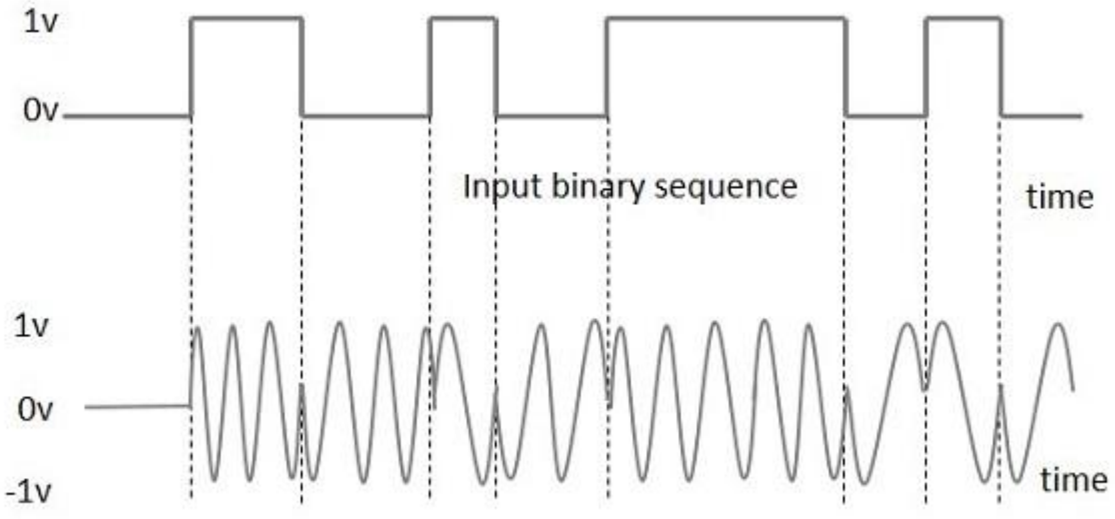
Binary Phase Shift Keying BPSK

This is also called as 2-phase PSK or Phase Reversal Keying. In this technique, the sine wave carrier takes two phase reversals such as 0° and 180°.

BPSK is basically a Double Side Band Suppressed Carrier DSBSC modulation scheme, for message being the digital information.

The modulation of BPSK is done using a balance modulator, which multiplies the two signals applied at the input. For a zero binary input, the phase will be **0°** and for a high input, the phase reversal is of **180°**.

Following is the diagrammatic representation of BPSK Modulated output wave along with its given input.

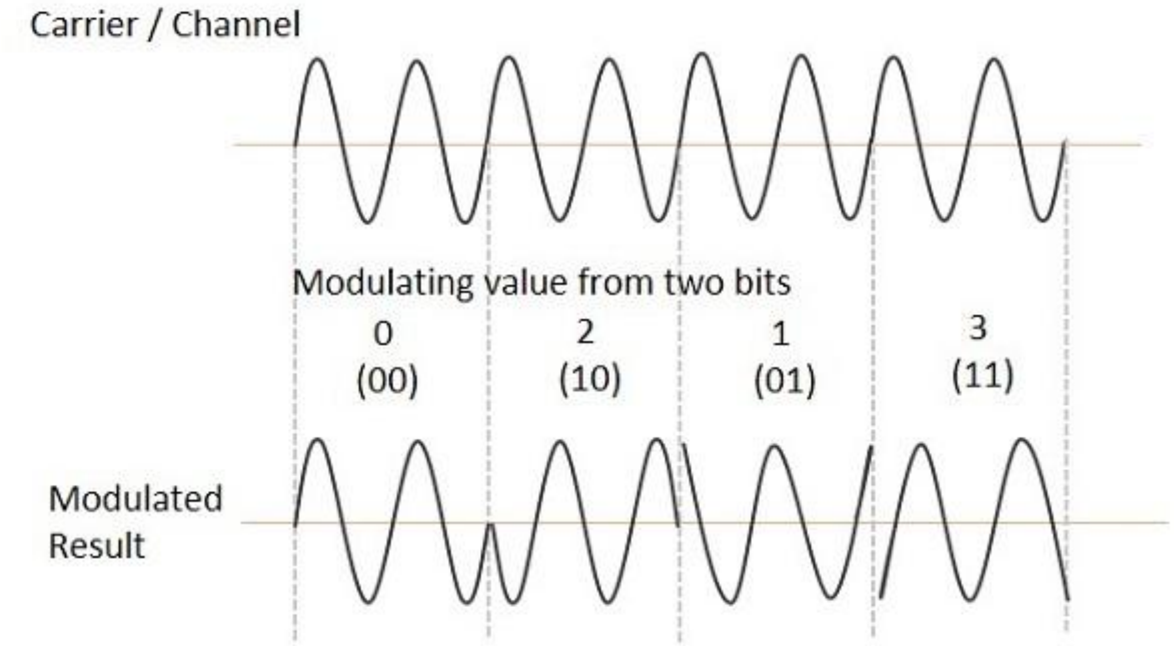


BPSK Modulated output wave

The **Quadrature Phase Shift Keying**

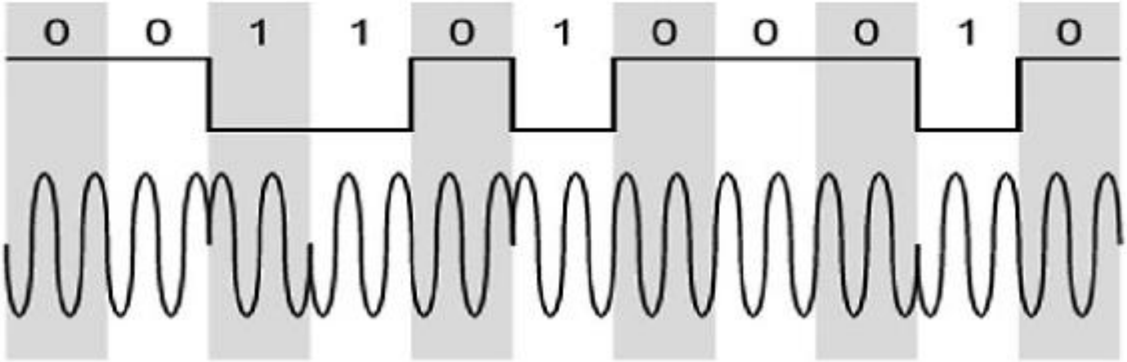
QPSK is a variation of BPSK, and it is also a Double Side Band Suppressed Carrier DSBSC modulation scheme, which sends two bits of digital information at a time, called as **bigits**.

The QPSK waveform for two-bits input is as follows, which shows the modulated result for different instances of binary inputs.



In **Differential Phase Shift Keying** DPSK���� the phase of the modulated signal is shifted relative to the previous signal element. No reference signal is considered here. The signal phase follows the high or low state of the previous element. This DPSK technique doesn't need a reference oscillator.

The following figure represents the model waveform of DPSK.



It is seen from the above figure that, if the data bit is Low i.e., 0, then the phase of the signal is not reversed, but continued as it was. If the data is a High i.e., 1, then the phase of the signal is reversed, as with NRZI, invert on 1 a form of differential encoding

If we observe the above waveform, we can say that the High state represents an **M** in the modulating signal and the Low state represents a **W** in the modulating signal.

UNIT-IV

ATM (Asynchronous Transfer Mode)

- Broadband ISDN (B-ISDN) is a set of communication protocols which are designed to transport a wide range of services simultaneously.
- The purpose of B-ISDN is to simplify and reduce the cost of communication between the interconnecting LAN's, multimedia conferencing, interactive games, image transmission etc.
- B-ISDN is the **low-level MAC(Media Access control) protocol** for transferring the actual data.

The ATM (Asynchronous Transfer Mode) was designed with an aim to provide:

1. High speed data rate.
2. Low error rate between two or more switching centers.
3. Digital voice and videos.
4. Low operating cost.

Features of ATM

- Flexibility and versatility of voice, videos and images can be transmitted simultaneously over a single or integrated corporate network.
- Higher transmission capability.
- It provides support for virtual networks.

ATM Bit Rates

ATM supports four different types of bit rate:

1. Constant bit rate (CBR)

- CBR traffic is derived from the source, where the information is transmitted at a constant rate. Example: Telephonic speech without silencer.

2. Variable Bit Rate (VBR)

- Variable traffic is derived from a variable source. Example: Compressed voice or video with silence suppression.

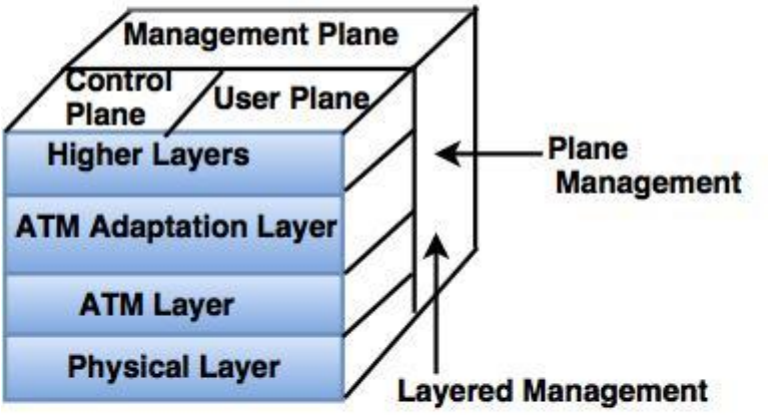
3. Available Bit Rate (VBR)

- When a carrier has allocated the necessary bandwidth on the links to carry CBR traffic and minimum VBR is guaranteed. The ABR is the mechanism to share the remaining bandwidth fairly between the links.

4. Unspecified Bit Rate (UBR)

- In **UBR,** there is no guarantee about the bandwidth traffic delay and loss. The control of flow in UBR can be provided from the end device.
- The protocol which performs the operation of braking frames into the cells is known as **ATM Adaptation Layer (AAL).**
- Cells carrying speech and video must be received in the order they were sent. This is known as preserving data integrity and it is a function of ATM layer.
- Any link which preserves the order of data entering and leaving is known as **channel.**
- In ATM protocols, an end-to end connection is established before traffic and starts to flow. Then ,the traffic follows the same path through the network to achieve a true quality of service.
- The connection-less services are implemented with the help of **AAL.**

Architecture of ATM



ATM Architecture

1. Physical layer

- Physical layer is a point-to-point transfer mechanism at the top of hardware (it may be wire also).
- Physical layer adds its own information to each cell which is transmitted for link management.

Physical layer performs four functions:

i) Physical layer converts bits into cells.

ii) It transmits and receives the bits on physical medium.

Iii) Tracks the cell boundaries.

iv) Packaging of cell into frames.

ATM layer is common to all services which can have the packet transfer capabilities.

2. ATM layer

- ATM layer provides the routing information to the data cells.
- ATM interfaces with the AAL and the Physical layer.
- Functions of ATM layer are under the network management, signaling and OAM protocol.

3. ATM Adaptation Layer

- AAL provides the flexibility of a single communication process to carry the multiple types of traffic such as data, voice, video and multimedia.
- **AAL** is divided into two major parts.
- Upper part of the AAL is called as the **convergence sublayer.** Its task is to provide the interface to the application. The lower part of the AAL is called as the segmentation and reassembly (SAR) sublayer. It can add headers and trailers to the data units given to it by the convergence sublayer to form cell payloads.

DISCOVER ABOUT TRANSMISSION OF ATM CELLS

It is an International Telecommunication Union- Telecommunications Standards Section (ITU-T) efficient for call relay and it transmits all information including multiple service types such as data, video, or voice which is conveyed in small fixed-size packets called cells.

Cells are transmitted asynchronously and the network is connection-oriented.

ATM is a technology that has some event in the development of broadband ISDN in the 1970s and 1980s, which can be considered an evolution of packet switching.

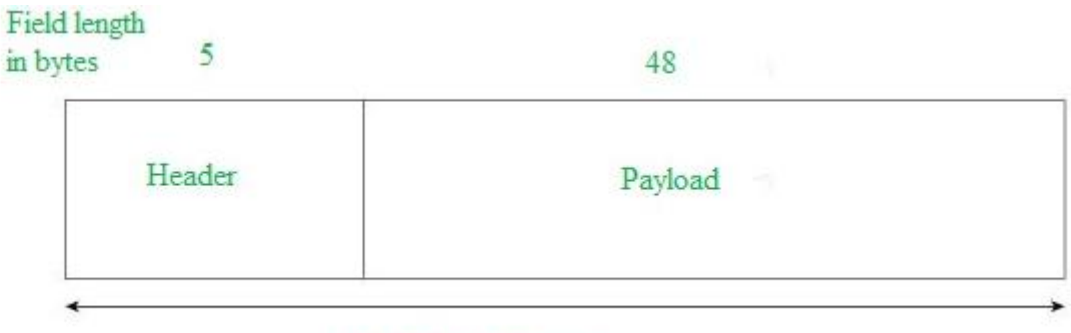
Thus it can carry multiple types of traffic with **end-to-end** quality of service. ATM is independent of a transmission medium, they may be sent on a wire or fiber by themselves or they may also be packaged inside the payload of other carrier systems.

ATM networks use "Packet" or "cell" Switching with virtual circuits. Its design helps in the implementation of high-performance multimedia networking. *Each cell is 53 bytes long* – 5 bytes header and 48 bytes payload. Making an ATM call requires first sending a message to set up a connection.

Subsequently, all cells follow the same path to the destination. It can handle both constant rate traffic and variable rate traffic.

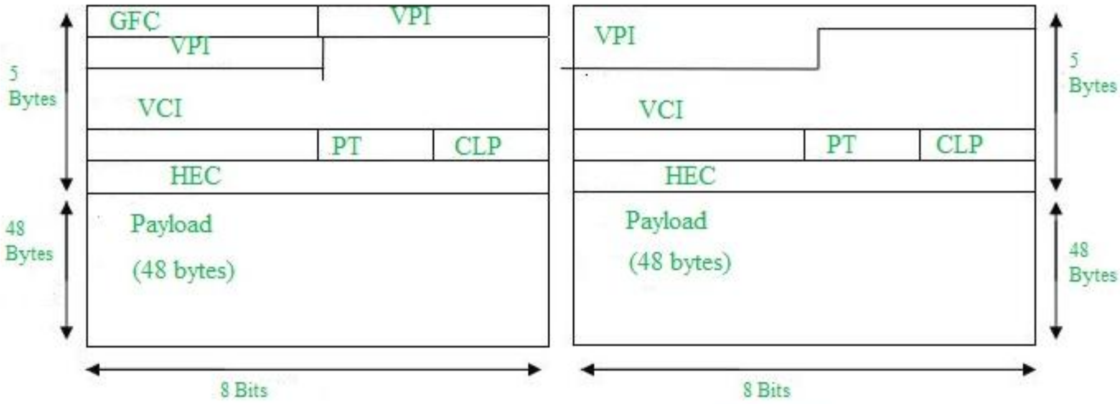
ATM CELL FORMAT –

As information is transmitted in ATM in the form of fixed-size units called **cells**. As known already each cell is 53 bytes long which consists of a 5 bytes header and 48 bytes payload.



ATM Cell Format

Asynchronous Transfer Mode can be of two format types which are as follows:



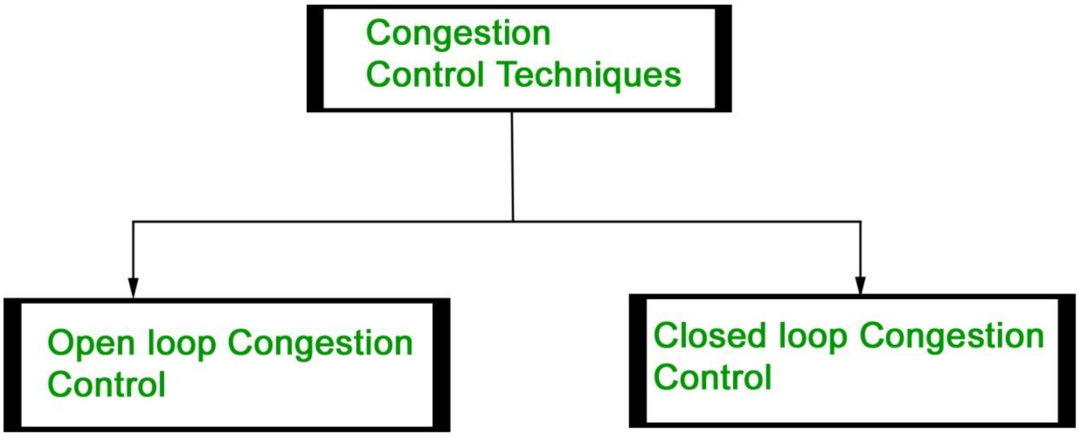
UNI Cell Format NNI Cell Format

1. **UNI Header:** This is used within private networks of ATMs for communication between ATM endpoints and ATM switches. It includes the Generic Flow Control (GFC) field.

2. **NNI Header:** is used for communication between ATM switches, and it does not include the Generic Flow Control(GFC) instead it includes a Virtual Path Identifier (VPI) which occupies the first 12 bits.

BUILD THE MECHANISMS FOR CONGESTION CONTROL

- Congestion control refers to the techniques used to control or prevent congestion.
- Congestion control techniques can be broadly classified into two categories:


Congestion Control Techniques
Open loop Congestion Control
Closed loop Congestion Control

Open Loop Congestion Control

Open loop congestion control policies are applied to prevent congestion before it happens. The congestion control is handled either by the source or the destination.

Policies adopted by open loop congestion control –

1. **Retransmission Policy :**
   It is the policy in which retransmission of the packets are taken care of. If the sender feels that a sent packet is lost or corrupted, the packet needs to be retransmitted. This transmission may increase the congestion in the network.
   To prevent congestion, retransmission timers must be designed to prevent congestion and also able to optimize efficiency.

2. **Window Policy :**
   The type of window at the sender's side may also affect the congestion. Several packets in the Go-back-n window are re-sent, although some packets may be received successfully at the receiver side. This duplication may increase the congestion in the network and make it worse.

3. **Discarding Policy :**
   A good discarding policy adopted by the routers is that the routers may prevent congestion and at the same time partially discard the corrupted or less sensitive packages and also be able to maintain the quality of a message.

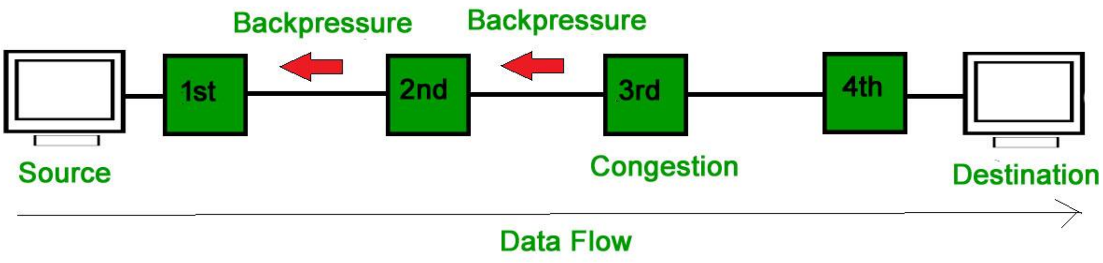
4. **Acknowledgment Policy :**
   Since acknowledgements are also the part of the load in the network, the acknowledgment policy imposed by the receiver may also affect congestion. Several approaches can be used to prevent congestion related to acknowledgment.
5. **Admission Policy :**
   In admission policy a mechanism should be used to prevent congestion. Switches in a flow should first check the resource requirement of a network flow before transmitting it further. If there is a chance of a congestion or there is a congestion in the network, router should deny establishing a virtual network connection to prevent further congestion.

Closed Loop Congestion Control

Closed loop congestion control techniques are used to treat or alleviate congestion after it happens. Several techniques are used by different protocols; some of them are:

1. Backpressure :

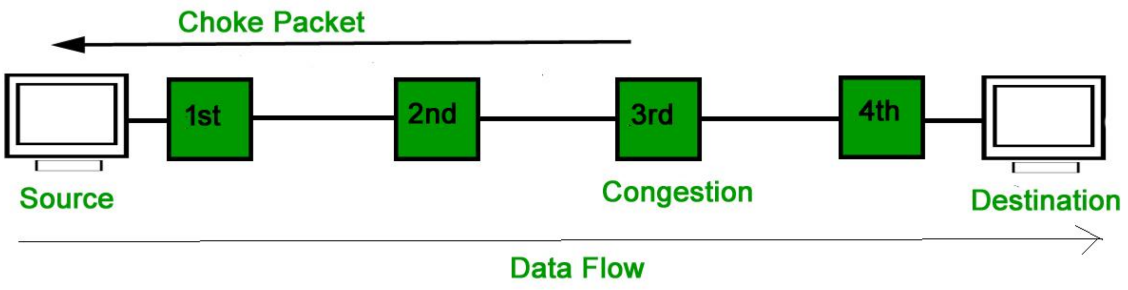
Backpressure is a technique in which a congested node stops receiving packets from upstream node. This may cause the upstream node or nodes to become congested and reject receiving data from above nodes. Backpressure is a node-to-node congestion control technique that propagate in the opposite direction of data flow. The backpressure technique can be applied only to virtual circuit where each node has information of its above upstream node.



In above diagram the 3rd node is congested and stops receiving packets as a result 2nd node may be get congested due to slowing down of the output data flow. Similarly 1st node may get congested and inform the source to slow down.

2. Choke Packet Technique :

Choke packet technique is applicable to both virtual networks as well as datagram subnets. A choke packet is a packet sent by a node to the source to inform it of congestion. Each router monitors its resources and the utilization at each of its output lines. Whenever the resource utilization exceeds the threshold value which is set by the administrator, the router directly sends a choke packet to the source giving it a feedback to reduce the traffic. The intermediate nodes through which the packets has traveled are not warned about congestion.



3. Implicit Signaling :

In implicit signaling, there is no communication between the congested nodes and the source. The source guesses that there is congestion in a network. For example when sender sends several packets and there is no acknowledgment for a while, one assumption is that there is a congestion.

4. Explicit Signaling :

In explicit signaling, if a node experiences congestion it can explicitly sends a packet to the source or destination to inform about congestion. The difference between choke packet and explicit signaling is that the signal is included in the packets that carry data rather than creating a different packet as in case of choke packet technique.

Forward Signaling : In forward signaling, a signal is sent in the direction of the congestion. The destination is warned about congestion. The receiver in this case adopt policies to prevent further congestion.

- **Backward Signaling :** In backward signaling, a signal is sent in the opposite direction of the congestion. The source is warned about congestion and it needs to slow down.