**UNIT-II**

**ERROR DETECTION AND CORRECTION:**

**INRODUCTION:**

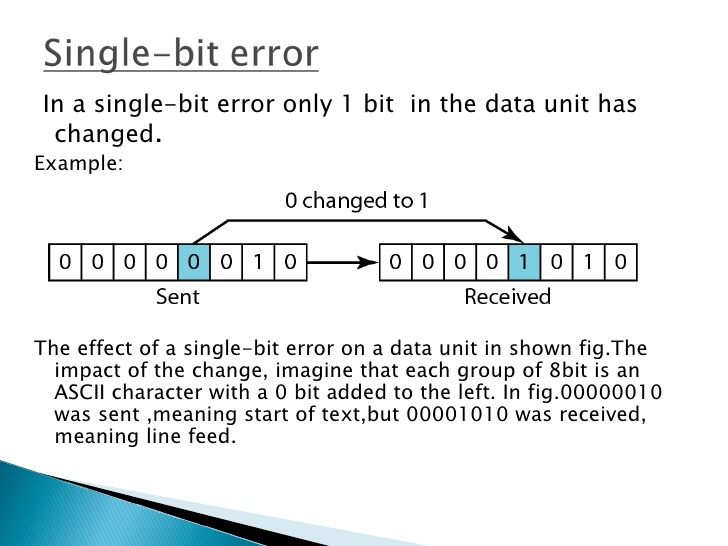
* Data can be corrupted during transmission, corrupted or modified data is known as error.
* Some application requires that errors to be detected and corrected.

**Types of error:**

* Bits flow from one point to another they are subject to unpredictable changes because of interference, this lead to change the shape of the signal.
* Single bit error
* Burst error

**Single bit error:**

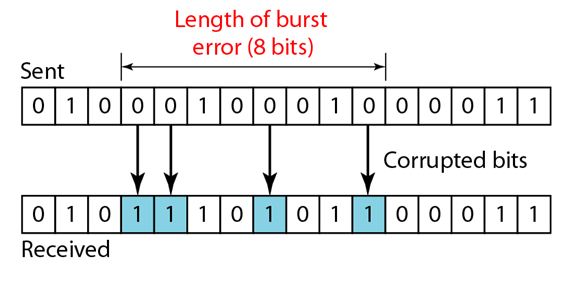
* It means that only one bit of a given data unit is changed from o to 1 or 1 to 0 (zero).



* From the above example we sent 00000010 (ASCII STX), Meaning start of text but 00001010 (ASCII LF) was received meaning is line feed.
* Single bit error may be appearing both serial data transmission and parallel data transmission.

**Burst errors:**

* It means that two or more bit in the data unit have changed from one to 0 (or) 0 to 1.
* The length of the burst is measured from the first corrupted to the last corrupted bit



* In the above example we sent be bit 0100010001000011, but we received the bit is 0101110101100011.
* The burst error does not necessary that the errors occur in consecutive bits.
* Burst error is most likely happen in a serial transmission.

**Redundancy:**

* To detect (or) correct errors, we need to send extra bit (redundant) with data.
* This redundant bit are added by the sender and removed by the receiver.
* The correction of errors is more difficult than the detection.
* In error correction, we need to know the exact number of bits that are corrected and more importantly, the location in the message.
* The number of the errors and the size of the message are important factors.

**Forward error correction and retransmission:**

* It is the process in which the receiver tries guess the message by using the redundant bit.
* This is possible, if the number of errors is small.

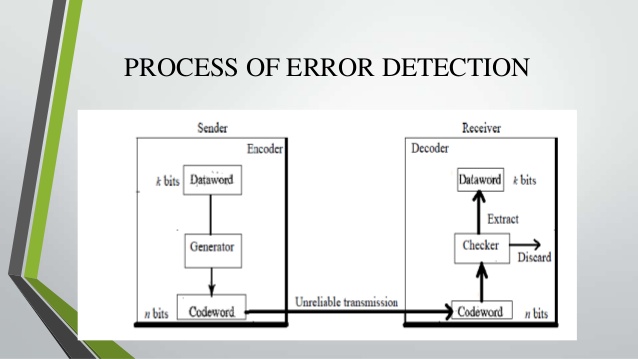
**Retransmission:**

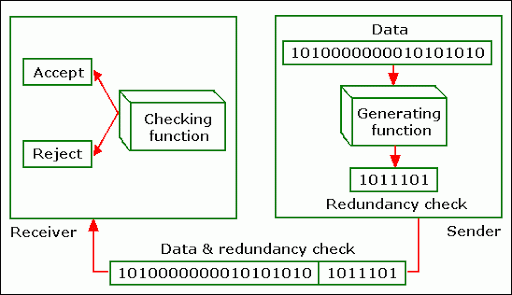
* Correction by retransmission is a technique in which the receiver detects the accurance of an error and asks the sender to resend the message.
* Resending is repeated until a message arrives that the receiver believes is error free.

**Coding (or) redundancy:**

* Redundancy is achieved through various coding schemes.

**Diagram:**





* In order to detect errors that make happen, the concepts of including extra bit determined, this technique is called redundancy, because the extra bit redundant to the information.
* Once the data system has been generated, it passes through a device that analyze it and add an appropriate code redundancy check.
* The receiver receive puts the entire data through a checking function.
* If a received bit stream passes the checking criteria, the data is accepted and the redundant bits are discarded.

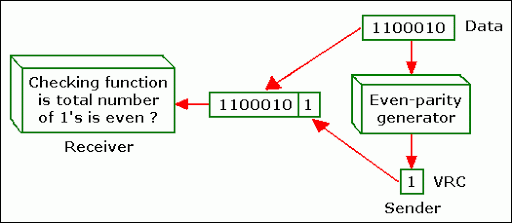
**Types of redundancy check:**

There are four types of redundancy check are used in data communication.

1. Vertical redundancy check(VRC)
2. Longitudinal redundancy check(LRC)
3. Cyclic redundancy check(CRC)
4. Checksum

**Vertical redundancy checks (VRC):**

* It is least expensive mechanism.
* It is also called parity check.
* In this technique the redundant bit called a parity bit is appended to every data unit so that the total 1s in the unit (including parity bit) becomes even.
* Ex: suppose we want to transmit the binary data unit.



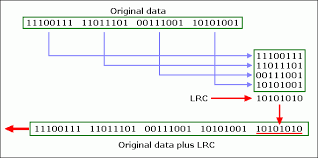
* Adding together the number of 1 ‘s gives as 3, an add number before transmitting we pass the data unit through a parity generator.
* The parity generator count the 1 and append to the parity bit to the end.
* The total number 1 ‘s is now an even number.
* The system now transmit the entire unit through on even parity checking function.
* If the receiver see 11000011, it count four is an even number and the data unit passes.

**Performance:**

* It can detect all single bit errors
* It can detect burst errors only if the total number of bit changed is odd (1,3,5,7).

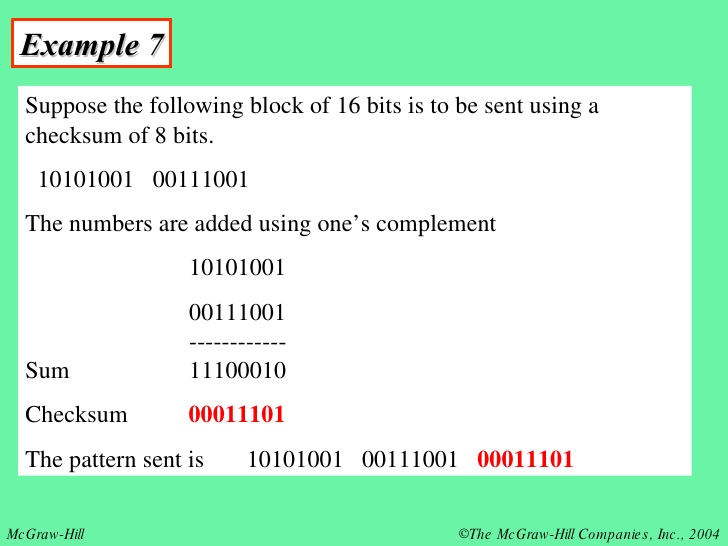
**Longitudinal redundancy check(LRC):**

* It is a two dimensional parity checker.
* Length data stored an table format.

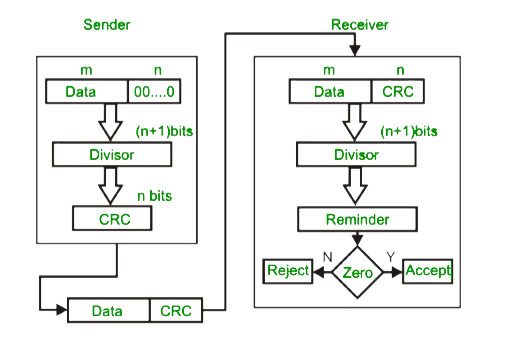


* Block of bit is divided in rows and a parity for each column is created and redundant row of bits is added to the whole block.

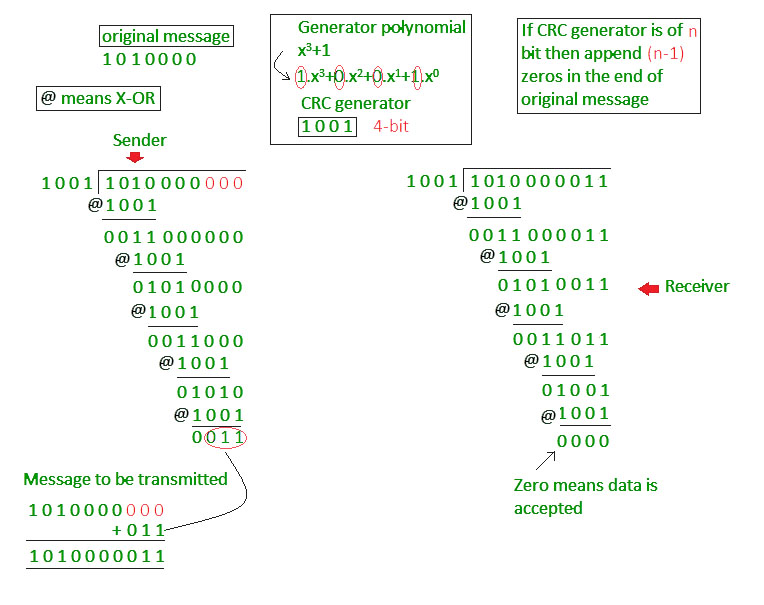
**Checksum redundancy check(CRC):**

****

**Cyclic Redundancy Check (CRC):**

****

* Message after three 0 bits appended
* Frame – 100100
* Generator – 1101



* The most powerful of the redundancy checking technique is cyclic redundancy checking it is also called polynomial code.
* The CRC is based on binary division, instead of adding bit to achieve to desired parity of sequence of redundant bit called the CRC.
* CRC is updated or appended to the end of the data unit so that the resulting data unit becomes exactly devisable by a second.

**CRC Performance:**

* CRC is a very effective error detection method.
* CRC can detect all burst errors, that affect on odd number of bits.
* CRC can detect all burst errors of length less than or equal to the degree of the polynomial.

**Data link layer:**

* The two main function of the data link layer are:

1. Data link control
2. Media access control

**Data link control:**

* It deal with the design and procedures for communication between two adjacent node (node- to –node communication).
* Data link control function include framing, flow control, error control and protocol

**Media access control:**

* How to share the link.

**Framing:**

* Data transmission in the physical layer means moving bit in form of a signal from the source to the destination.
* Framing in the data link layer separate a message from one source to a destination by adding a sender address and a destination address.

**There are two category are available,**

1. Fixed size framing.
2. Variable size framing.

**Fixed size framing:**

* In this type of framing there is no need for defining the boundaries, of the frame, the size excess can be used as a delimiter.

**Variable size framing:**

* In this method, we need a way to define the end of the frame and the beginning of the next.
* To approaches are used for this purpose.

1. Character oriented approach
2. Bit oriented approach.

**Flow control:**

* Flow control refers to a set of procedures used for restrict the amount of data that the sender can send before waiting for acknowledgement.
* Flow control is a set of procedures that tells the sender how much data it can transmit before it must wait for an acknowledgement from the receiver.
* Any receiving device has a limited speed at which it can process incoming data limited amount of memory in which to store incoming data.

**Error control:**

* Error control in the data link layer is based on automatic repeat request, which is the retransmission of data.
* Error control is both error detection and correction.
* It allows the receiver to inform the sender of any frames last in transmission and co-ordinates the retransmission of those frames by the sender.
* Any time an error is detected in an exchange, specified frames are retransmitted, this process is called automatic repeat request (ARQ).

**Protocols:**

* Set of rules and regulation about the communication network.

1. For noiseless channel (SIMPLEX, STOP - AND - WAIT).
2. For noisy channel(STOP–AND–WAIT-ARQ, GO-BACK–N-ARQ, SELECTIVE-REPEAT-ARQ)

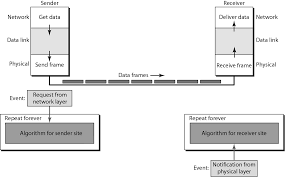
**For noiseless channel:**

1. Simplex

2. Stop-and –wait.

**Simplex**

* In this type of channels in which no frames are lost, duplicated or corrupted.



* Data are transmission in one directional only both the transmitting and receiving network layers are always ready.
* Processing time can be ignored, infinite buffer space is available.
* The communication channel between the data link layer never are layer of frames.
* In this protocol consist of two, distinct procedures for sender and receiver.
* The sender runs in the data link layer of source machine and the receiver runs in the data link layer of the destination machine.
* In this method sequence, number, acknowledgement number are not used.
* Similar to simplex physical channel.

**Algorithm:**

Sender side:

While (true)

{

Wait for event();

If(event (request to send)

{

Get data();

Make frame();

Send frame();

} }

**Receiver side:**

While (true)

{

Wait for event ();

If(event (arrival notification))

{

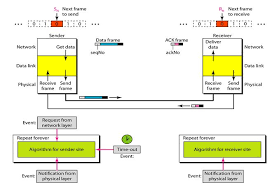
Receive frame();

Extract data();

Deliver data();

} }

**Stop and wait protocol:**

****

* In this protocol have the receiver provide feedback to the sender.
* After having passed a packet to its network layer, the receiver sends a little dummy frame, back to the sender that means permission to transmit the next frame.
* Protocols in which the sender send one frame and then wait for an acknowledgement before proceeding are called stop and wait.
* Frames do travel in both direction communication channel between the data link layers need to the capable of bidirectional information transmit.
* Sender send the frame, receiver send a frame then the sender send the another frame, the receiver send another one.
* A half, duplex physical channel is achieve.

**Algorithm:**

**Sender Side:**

While (true)

Can send = true;

{

Wait for event();

If(event (request to send)AND can send)

{

Get data();

Make frame;

Send frame;

Can send =false;

}

Wait for event();

If(event (arrival notification))

{

Receive frame();

Can send = true;

}

}

**Receiver side:**

While(true)

{

Wait for event();

If(event (arrival notification))

{

Receive frame();

Extract data();

Send frame();

}

}

**For noisy channel:**

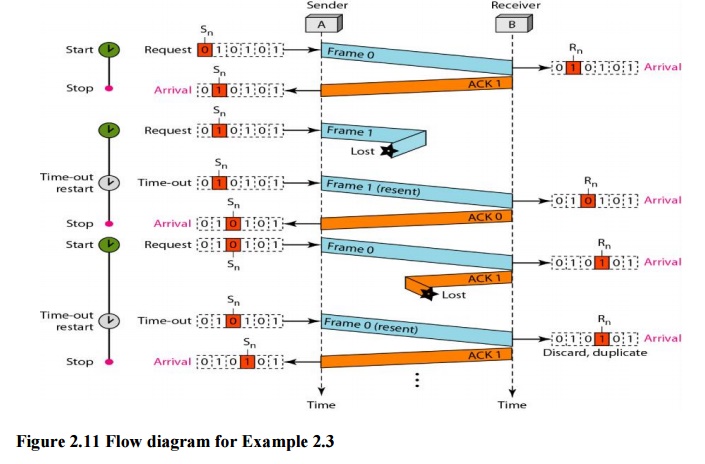
1. Stop – and – wait- ARQ
2. Go – back – n ARQ,
3. Selective repeat ARQ

**Stop and wait ARQ:**

* IF add a simple error control mechanism to the stop-and –wait-protocol.
* To detect and correct corrupted frames, we need to add a redundancy bits to our data frames, when the frame arrives at the receiver side, it is checked and if it is corrupted it is silently discarded.
* In our previous protocols, there was no way to identify a frame, the received frame could be correct one or a duplicate or a frame out of order, the solution is to number the frames.
* The corrupt and last frames need to be resend in this protocol.
* The sender keeps a copy of the send frame, at the same time it start a timer, if the timer expires and there is no acknowledgement for the send frame, the frame is resend and the timer is start.

**Sequence number:**

* The frame arrive safe and sound at the receiver side, the receiver send on ACK, the ACK arrive at the sender side, causing the sender to send the next frame numbered x+1.
* The frame arrive safe and sound at the receiver side, the receiver send on ACK but the ACK is corrupted (or) loss, the sender resend the frame (number x) after the timeout note that the frame here is a duplicate the receiver can recognize this fact because it expect frame x+1, but frame x was received.
* The frame is corrupted or never arrives at the receiver side, the sender resend the frame after the time out.



**Sender side algorithm:**

N=0

Can send=1,

While(true)

{

Wait for event();

If(event(request to send)and can send)

{

Get data();

Make frame(sn);

Store frame(sn);

Send frame(sn);

Start timer=();

Sn=sn+1;

Can send =false;

}

Wait for event();

If(event (arrival notification)

{

If (nt corrupted and ack no)

{

Stop timer();

Pure frame sn+1;

Can send =true;

} }

If (event (time out))

{

Start timer();

Resend frame(sn-1);

}

**Receiver side:**

N=0;

While(true)

{

Wait – for event();

If (event(arrival notification)

{

Receive frame();

If (corrupted frame==I;

Sleep();

If(seq no==rn)

{

Extract data();

Deliver data();

Rn=rn+1;

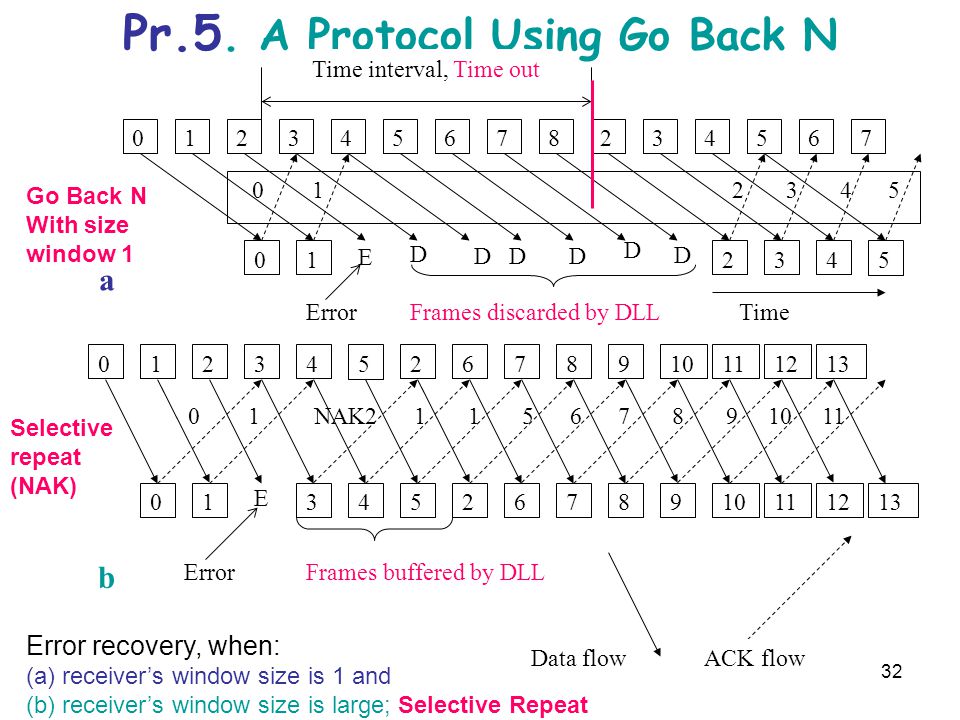
Send frame(rn);

}

}

**GO BACK N ARQ PROTOCOL:**

* A problem is a sender to wait for an ACK before sending another frame.
* If we relax the restriction much better effectively, can be achieved.
* The solution is allowing the sender to transmit up to ‘w’ frames before blocking instead of just one.
* If a frame in the middle of a long stream is damage or loss large number of succeeding frames will be arrive at the receiver, the sender even find out that anything is wrong.
* When a damaged frame arrive receiver it should be discarded.
* The receiver simply to discarded all sub sequent frames, sending no ACK for the discarded frame.
* The data link layer return to accept any frame expect next one.
* Next the senders will timeout and the retransmit all un ACK in order. Starting with the damaged one.

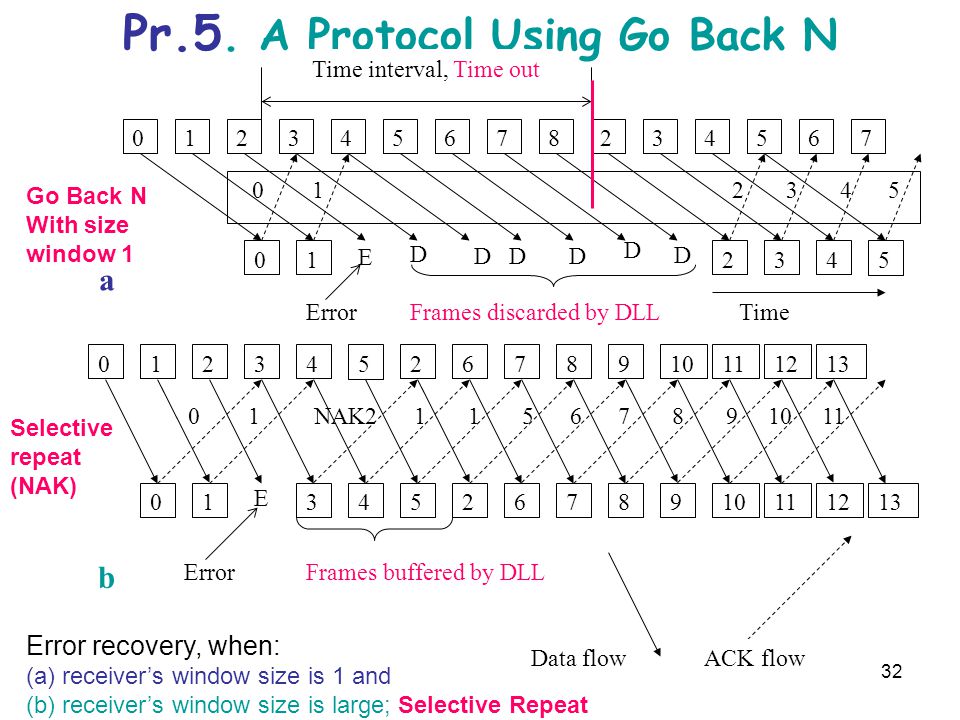


**Piggy backing:**

* The technique of temporarily delay in outgoing ACK, so that they can be hooked on to the next outgoing data frame is known as piggy backing.
* In the above example frame 0 and 1 are correctly received and Acknowledged, frame 2 is damaged or loss.
* The sender unaware of this, problem, continues to send frame until the timer expires then if backs up to frame 2 and start all over with it sending 2,3,4 …. All over again.

**Selective repeat ARQ:**

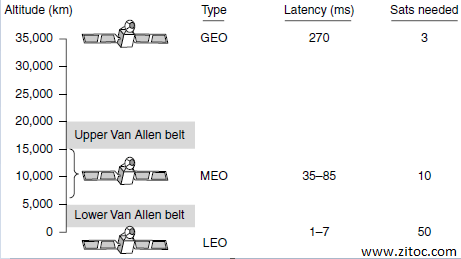
* General strategy for handling errors when frames are pipelined is called selective repeat ARQ.
* In this techniques a bad frame that is received is discarded but good frames received after it are buffered.
* When the senders timeout, only the oldest unacknowledged frame is retransmitted
* If the frames arrived correctly, the receiver can delivered to the network layer in sequence.



* Selective repeat is often, compiled with having the receiver send a (NACK) when it detect an error.
* Stimulate retransmission before the corresponding timer expire and thus improve performance.
* Frames 0 and 1 are correctly received and Acknowledged, frame 2 is lost.
* When frame 3 is arrives at the receiver the data link layer notices a missed frame and send NAK to sender.
* Next frame 4 and 5 arrives, the two are buffered by the data link, layer the NAK to get back to the sender which immediately resend frame 2, when that arrives, the data link layer now has 2,3, 4,and 5 can was all of them to the network layer in the correct order.

**Communication satellite:**

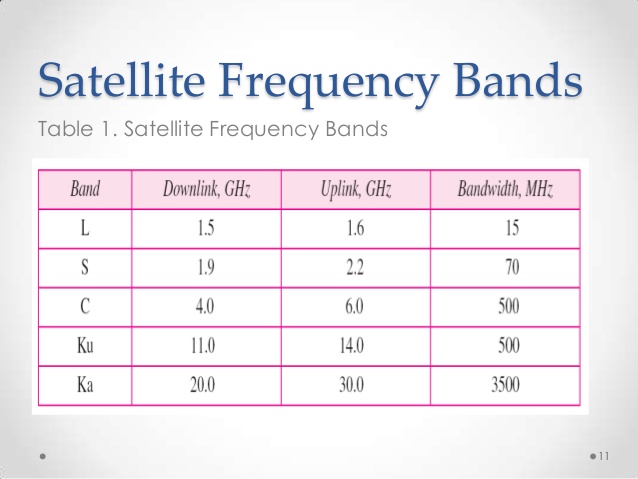
1. Geostationary satellite
2. Medium earth orbit satellite
3. Low earth orbit satellite



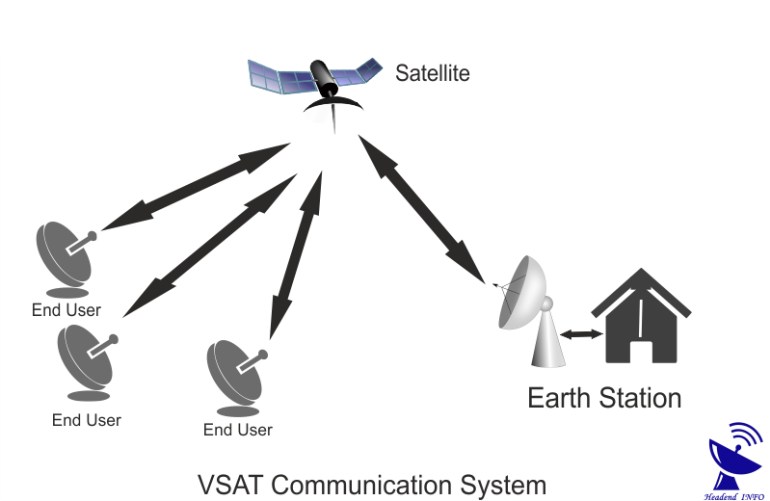
**Geostationary satellite:**

* Geostationary satellite contains orbit, solar panel, radio frequency and launching procedures.
* Communication satellite has become a multibillion dollar business and the only aspect of outer space that has become highly profitable.
* The high flying satellite is called geo satellite (geostationary earth orbit).
* Modern satellite can be quite large, weight up to 4000 kg and consume several kilo watt of electric power produce by the solar power.
* The electric of solar planetary, gravity tent to move them away from their assigned orbits slot and orientation, this fine tuning activities called station keeping.
* Orbits slot and frequency are bone of the connection.

**Satellite bandwidth:**



* The main band is c band that was the first to be designed commercial satellite traffic.
* Two traffic frequency ranges are assigned it, the lower one for down link traffic and the upper one for up link traffic.
* To allow traffic to go both ways at the same time.
* The first geostationary satellite had a single spatial beam that eliminated about 1/3 of the earth surface called its foot print.



* A new development in the communication satellite world is the development of low cost micro station called VSAT.
* This terminal have one meter are smaller antenna and carryout about 1(one) watt of power.
* In many VSAT system, the micro station do not have enough power to communicate directly with one another, instead a special ground station the HUB is used.

**Medium earth orbit satellite:**

* It is placed In much lower altitude.
* They have smaller foot print on the ground and require less powerful transmitter to reach them.
* They are not using telecommunication.

**Low earth orbit satellite:**

* Moving down in altitude become to the LEO satellite the satellite is so closed to the earth.
* The ground station do not need much power

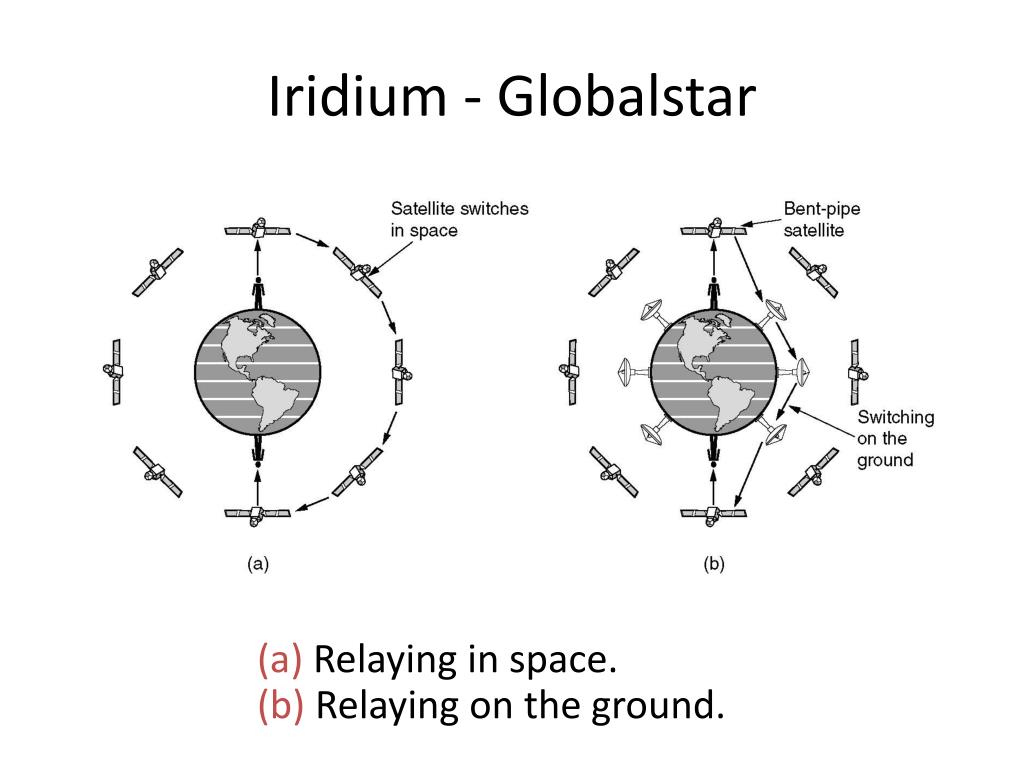
**Types:**

1. Iridium - voice communication
2. Global star -voice communication
3. Tele desic -internet

**Iridium :**

* Launching satellite in the year 1997 but communication service start in November 1998.
* It provide worldwide telecommunication service using hand held device that communication directly.
* It provide voice, data paging and fax services everywhere on the land, sea, and air.
* The iridium satellite is positioned at altitude of 750 KMs they are arranged in north south necklace.
* 6 satellite necklaces cover the entire earth. Each satellite has a maximum of 48 cells, with a total of 1628 cells cover the surface of the earth.

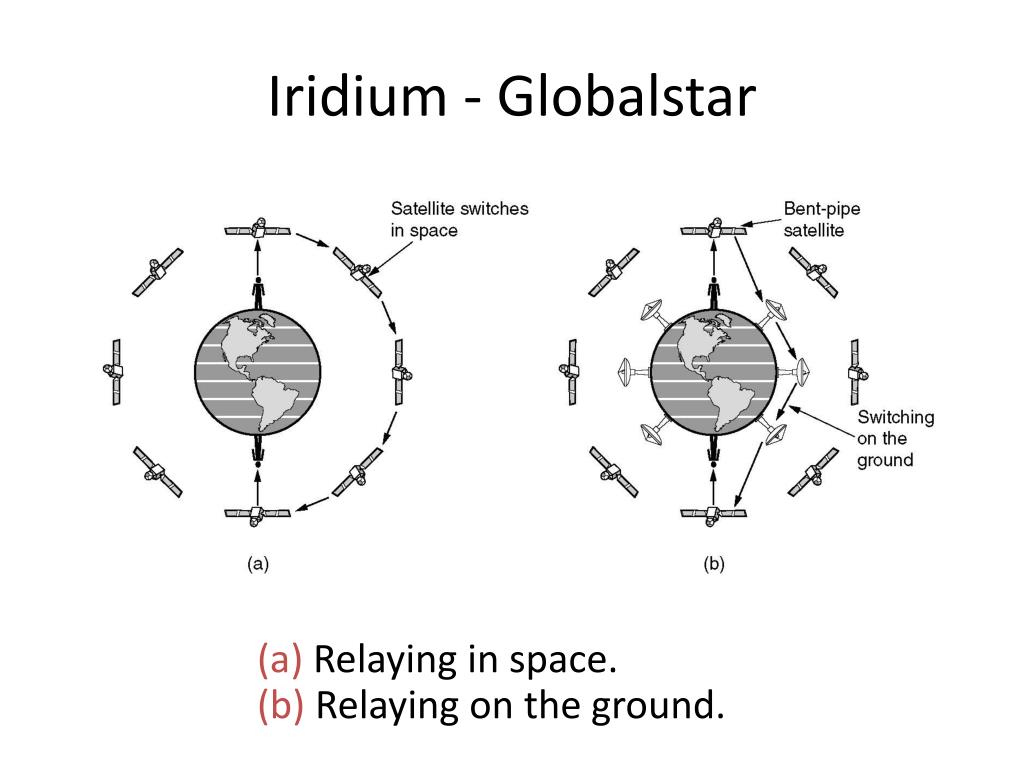




* The main properties are direct connection to satellite to satellite.

**Global star:**

* An alternative design to iridium is global star, it is based on 48 LEO satellite and used a different switching scheme.
* Global star used a bend pipe design to communicate satellite to satellite.



**Tele desic:**

* It is targeted an internet user all over the world.
* The goal of the system is to provide millions of concurrent internet users to access the system.
* It is also provide high band width to computer user.
* The system consists of 88 small foot print satellite arranged in twelve manner later it is changed width 30 satellite with larger footprint.

**RANDOM ACCESS**

In random access or contention methods, no station is superior to another station and none is assigned the control over another. No station permits, or does not permit, another station to send.

At each instance, a station that has data to send uses a procedure defined by the protocol to make a decision on whether or not to send. This decision depends on the state of the medium (idle or busy).

Two features give this method its name.

First, there is no scheduled time for a station to transmit. Transmission is random among the stations. That is why these methods are called *random access.*

Second, no rules specify which station should send next. Stations compete with one another to access the medium. That is why these methods are also called *contention* methods.

The method was improved with the addition of a procedure that forces the station to sense the medium before transmitting. This was called carrier sense multiple access. This method later evolved into two parallel methods: carrier sense multiple access with collision detection (CSMA/CD) and carrier sense multiple access with collision avoidance *(CSMA/CA). CSMA/CD* tells the station what to do when a collision is detected. *CSMA/CA* tries to avoid the collision.

**ALOHA**

ALOHA, the earliest random access method, was developed at the University of Hawaii in early 1970. It was designed for a radio (wireless) LAN, but it can be used on any shared medium.

***Pure ALOHA***

The original ALOHA protocol is called pure ALOHA. This is a simple, but elegant protocol. The idea is that each station sends a frame whenever it has a frame to send. However, since there is only one channel to share, there is the possibility of collision between frames from different stations.

There are four stations (unrealistic assumption) that contend with one another for access to the shared channel. The figure shows that each station sends two frames; there are a total of eight frames on the shared medium. Some of these frames collide because multiple frames are in contention for the shared channel.

The pure ALOHA protocol relies on acknowledgments from the receiver. When a station sends a frame, it expects the receiver to send an acknowledgment. If the acknowledgment does not arrive after a time-out period, the station assumes that the frame (or the acknowledgment) has been destroyed and resends the frame.

**Carrier Sense Multiple Access (CSMA)**

To minimize the chance of collision and increase the performance, the CSMA method was developed. Carrier sense multiple access (CSMA) requires that each station first listen to the medium (or check the state of the medium) before sending.

***Vulnerable Time***

The vulnerable time for CSMA is the propagation time *Tp.* This is the time needed for a signal to propagate from one end of the medium to the other. When a station sends a frame, and any other station tries to send a frame during this time, a collision will result.

**Carrier Sense Multiple Access with Collision Detection (CSMA/CD)**

The CSMA method does not specify the procedure following a collision. Carrier sense multiple access with collision detection (CSMA/CD) augments the algorithm to handle the collision.

In this method, a station monitors the medium after it sends a frame to see if the transmission was successful. If so, the station is finished. If, however, there is a collision, the frame is sent again.

***Minimum Frame Size***

For *CSMAlCD* to work, we need a restriction on the frame size. Before sending the last bit of the frame, the sending station must detect a collision, if any, and abort the transmission.

**Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)**

The basic idea behind *CSMA/CD* is that a station needs to be able to receive while transmitting to detect a collision. When there is no collision, the station receives one signal: its own signal. When there is a collision, the station receives two signals: its own signal and the signal transmitted by a second station.

**CONTROLLED ACCESS**

In controlled access, the stations consult one another to find which station has the right to send. A station cannot send unless it has been authorized by other stations. We discuss four popular controlled-access methods.

**Reservation**

In the reservation method, a station needs to make a reservation before sending data. Time is divided into intervals. In each interval, a reservation frame precedes the data frames sent in that interval.

**Polling**

Polling works with topologies in which one device is designated as a primary station and the other devices are secondary stations. All data exchanges must be made through the primary device even when the ultimate destination is a secondary device.

***Select***

The *select* function is used whenever the primary device has something to send.. If the primary is neither sending nor receiving data, it knows the link is available.

**Token Passing**

In the token-passing method, the stations in a network are organized in a logical ring. In other words, for each station, there is a *predecessor* and a *successor.*

**IEEE 802.11**

IEEE has defined the specifications for a wireless LAN, called IEEE 802.11, which covers the physical and data link layers.

**Architecture**

The standard defines two kinds of services: the basic service set (BSS) and the extended service set (ESS).

***Basic Service Set***

IEEE 802.11 defines the basic service set (BSS) as the building block of a wireless LAN. A basic service set is made of stationary or mobile wireless stations and an optional central base station, known as the access point (AP).

The BSS without an AP is a stand-alone network and cannot send data to other BSSs. It is called an *ad hoc architecture.* In this architecture, stations can form a network without the need of an AP.

***Extended Service Set***

An extended service set (ESS) is made up of two or more BSSs with APs. In this case, the BSSs are connected through a *distribution system,* which is usually a wired LAN.

***Station Types***

IEEE 802.11 defines three types of stations based on their mobility in a wireless LAN:

**no-transition, BSS·transition, and ESS-transition mobility.**

A station with no-transition mobility is either stationary (not moving) or moving only inside a BSS.

A station with BSS-transition mobility can move from one BSS to another.

A station with ESS-transition mobility can move from one ESS to another.

**BLUETOOTH**

Bluetooth is a wireless LAN technology designed to connect devices of different functions such as telephones, notebooks, computers (desktop and laptop), cameras, printers, coffee makers, and so on.

A Bluetooth LAN is an ad hoc network.

Bluetooth technology has several applications. Peripheral devices such as a wire-less mouse or keyboard can communicate with the computer through this technology. Monitoring devices can communicate with sensor devices in a small health care center. Home security devices can use this technology to connect different sensors to the main security controller. Conference attendees can synchronize their laptop computers at a conference.

Bluetooth was originally started as a project by the Ericsson Company. It is named for Harald Blaatand, the king of Denmark (940-981) who united Denmark and Norway. *Blaatand* translates to *Bluetooth* in English.

Today, Bluetooth technology is the implementation of a protocol defined by the IEEE 802.15 standard. The standard defines a wireless personal-area network (PAN) operable in an area the size of a room or a hall.

**Architecture**

Bluetooth defines two types of networks: piconet and scatternet.

***Piconets***

A Bluetooth network is called a piconet, or a small net. A piconet can have up to eight stations, one of which is called the primary; the rest are called secondaries. Note that a piconet can have only one primary station. The communication between the primary and the secondary can be one-to-one or one-to-many.

***Scatternet***

Piconets can be combined to form what is called a scatternet. A secondary station in one piconet can be the primary in another piconet. This station can receive messages from the primary in the first piconet (as a secondary) and, acting as a primary, deliver them to secondaries in the second piconet. A station can be a member of two piconets.

***Bluetooth Devices***

1. Bluetooth device has a built-in short-range radio transmitter. The current data rate is 1 Mbps with a 2.4-GHz bandwidth.

**CONNECTING DEVICES**

The five categories contain devices which can be defined as

* Those which operate below the physical layer such as a passive hub.
* Those which operate at the physical layer (a repeater or an active hub).
* Those which operate at the physical and data link layers (a bridge or a two-layer switch).
* Those which operate at the physical, data link, and network layers (a router or a three-layer switch).
* Those which can operate at all five layers (a gateway).

**Passive Hubs**

A passive hub is just a connector. It connects the wires coming from different branches. In a star-topology Ethernet LAN, a passive hub is just a point where the signals coming from different stations collide; the hub is the collision point. This type of a hub is part of the media; its location in the Internet model is below the physical layer.

**Repeaters**

A repeater is a device that operates only in the physical layer. Signals that carry information within a network can travel a fixed distance before attenuation endangers the integrity of the data. A repeater receives a signal and, before it becomes too weak or corrupted, regenerates the original bit pattern. The repeater then sends the refreshed signal. A repeater can extend the physical length of a LAN.

**Active Hubs**

An active hub is actually a multipart repeater. It is normally used to create connections between stations in a physical star topology. Hubs can also be used to create multiple levels of hierarchy

**Bridges**

A bridge operates in both the physical and the data link layer. As a physical layer device, it regenerates the signal it receives. As a data link layer device, the bridge can check the physical (MAC) addresses (source and destination) contained in the frame.

**Routers**

A router is a three-layer device that routes packets based on their logical addresses (host-to-host addressing). A router normally connects LANs and WANs in the Internet and has a routing table that is used for making decisions about the route. The routing tables are normally dynamic and are updated using routing protocols.

**Gateway**

A gateway is normally a computer that operates in all five layers of the Internet or seven layers of OSI model. A gateway takes an application message, reads it, and interprets it. This means that it can be used as a connecting device between two internetworks that use different models.

**CELLULAR TELEPHONY**

Cellular telephony is designed to provide communications between two moving units, called mobile stations (MSs), or between one mobile unit and one stationary unit, often called a land unit. A service provider must be able to locate and track a caller, assign a channel to the call, and transfer the channel from base station to base station as the caller moves out of range.

To make this tracking possible, each cellular service area is divided into small regions called cells. Each cell contains an antenna and is controlled by a solar or AC powered network station, called the base station (BS). Each base station, in turn is controlled by a switching office, called a mobile switching center (MSC).

**Transmitting**

To place a call from a mobile station, the caller enters a code of 7 or 10 digits (a phone number) and presses the send button. The mobile station then scans the band, seeking a setup channel with a strong signal, and sends the data (phone number) to the closest base station using that channel. The base station relays the data to the MSC. The MSC sends the data on to the telephone central office. If the called party is available, a connection is made and the result is relayed back to the MSC

**Receiving**

When a mobile phone is called, the telephone central office sends the number to the MSC. The MSC searches for the location of the mobile station by sending query signals to each cell in a process called *paging.* Once the mobile station is found, the MSC transmits a ringing signal and, when the mobile station answers, assigns a voice channel to the call, allowing voice communication to begin.

**Roaming**

One feature of cellular telephony is called roaming. Roaming means, in principle, that a user can have access to communication or can be reached where there is coverage. A service provider usually has limited coverage. Neighboring service providers can pro-vide extended coverage through a roaming contract. The situation is similar to snail mail between countries. The charge for delivery of a letter between two countries can be divided upon agreement by the two countries.

**First Generation**

The first generation was designed for voice communication using analog signals. We discuss one first-generation mobile system used in North America, AMPS.

***AMPS***

Advanced **Mobile Phone** System (AMPS) is one of the leading analog cellular systems in North America. It uses FDMA to separate channels in a link.

Bands AMPS operates in the ISM 800-MHz band. The system uses two separate analog channels, one for forward (base station to mobile station) communication and one for reverse (mobile station to base station) communication. The band between 824 and 849 MHz carries reverse communication; the band between 869 and 894 MHz carries forward communication.

**Second Generation**

To provide higher-quality (less noise-prone) mobile voice communications, the second generation of the cellular phone network was developed. While the first generation was designed for analog voice communication, the second generation was mainly designed for digitized voice. Three major systems evolved in the second generation.

***D-AMPS***

The product of the evolution of the analog AMPS into a digital system is digital AMPS (D-AMPS). D-AMPS was designed to be backward-compatible with AMPS. This means that in a cell, one telephone can use AMPS and another D-AMPS. D-AMPS was first defined by IS-54 (Interim Standard 54) and later revised by IS-136.

***GSM***

The Global System for Mobile Communication (GSM) is a European standard that was developed to provide a common second-generation technology for all Europe. The aim was to replace a number of incompatible first-generation technologies.

**Third Generation**

The third generation of cellular telephony refers to a combination of technologies that provide a variety of services. The third generation can provide both digital data and voice communication. Using a small portable device, a person should be able to talk to anyone else in the world with a voice quality similar to that of the existing fixed telephone network. A person can download and watch a movie, can download and listen to music, can surf the Internet or play games, can have a video conference, and can do much more. One of the interesting characteristics of a third-generation system is that the portable device is always connected; you do not need to dial a number to connect to the Internet.

* Voice quality comparable to that of the existing public telephone network.
* Data rate of 144 kbps for access in a moving vehicle (car), 384 kbps for access as the user walks (pedestrians), and 2 Mbps for the stationary user (office or home).
* Support for packet-switched and circuit-switched data services.
* The main goal of third-generation cellular telephony is to provide universal personal communication.