Subject Name: Data Communication

Sardar Patel University Balaghat(M.P)

School of Engineering & Technology

Department of CSE

Subject Name: Data Communication

Subject Code: CSE501

Semester: 5th

Unit-I

DATA COMMUNICATION

Data Communication is a process of exchanging data or information. In case of computer networks this exchange is done between two devices over a transmission medium. This process involves a communication system which is made up of hardware and software. The hardware part involves the sender and receiver devices and the intermediate devices through which the data passes. The software part involves certain rules which specify what is to be communicated, how it is to be communicated and when. It is also called as a Protocol. The following sections describes the fundamental characteristics that are important for the effective working of data communication process and is followed by the components that make up a data communications system.

Characteristics of Data Communication

The effectiveness of any data communications system depends upon the following four fundamental characteristics:

1. Delivery: The data should be delivered to the correct destination and correct user.
2. Accuracy: The communication system should deliver the data accurately, without introducing any errors. The data may get corrupted during transmission affecting the accuracy of the delivered data.
3. Timeliness: Audio and Video data has to be delivered in a timely manner without any delay; such a data delivery is called real time transmission of data.
4. Jitter: It is the variation in the packet arrival time. Uneven Jitter may affect the timeliness of data being transmitted.

Components of Data Communication

A Data Communication system has five components as shown in the diagram below:

1. Message:- Message is the information to be communicated by the sender to the receiver.
2. Sender :-The sender is any device that is capable of sending the data (message).
3. Receiver:- The receiver is a device that the sender wants to communicate the data (message).
4. Transmission Medium:- It is the path by which the message travels from sender to receiver. It can be wired or wireless and many subtypes in both.
5. Protocol:- It is an agreed upon set or rules used by the sender and receiver to communicate data. A protocol is a set of rules that governs data communication. A Protocol is a necessity in data communications without which the communicating entities are like two persons trying to talk to each other in a different language without know the other language.

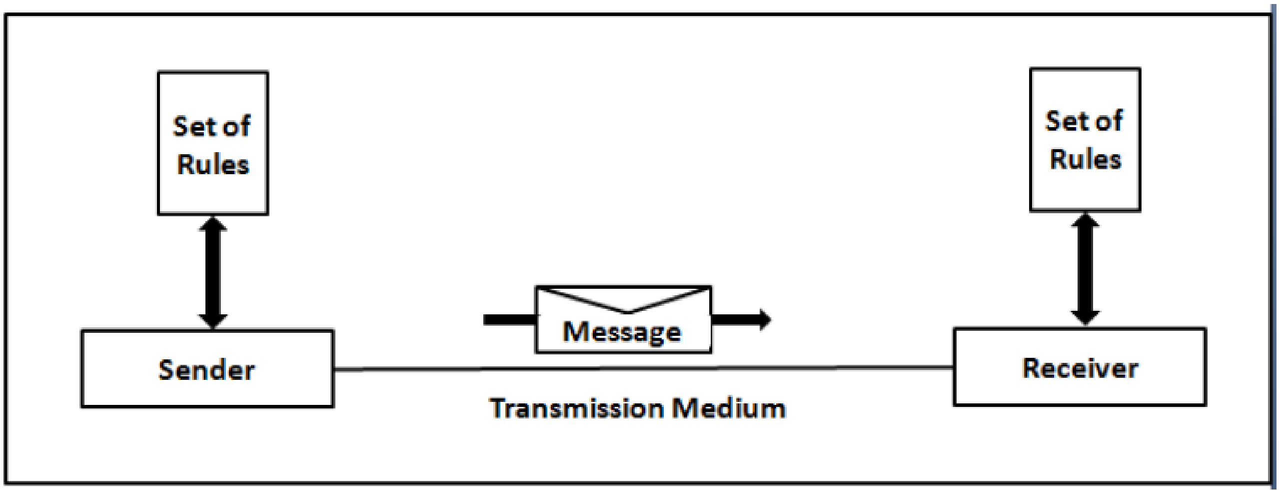


Fig. Components of a Data Communication System

Fig 1.1

DATA REPRESENTATION

Data is collection of raw facts which is processed to deduce information. There may be different forms in which data may be represented. Some of the forms of data used in communications are as follows:

1. Text -Text includes combination of alphabets in small case as well as upper case. It is stored as a pattern of bits. Prevalent encoding system : ASCII, Unicode
2. Numbers- Numbers include combination of digits from 0 to 9. It is stored as a pattern of bits. Prevalent encoding system : ASCII, Unicode
3. Images- An image is worth a thousand words‖ is a very famous saying. In computers images are digitally stored. A Pixel is the smallest element of an image. To put it in simple terms, a picture or image is a matrix of pixel elements. The pixels are represented in the form of bits. Depending upon the type of image (black n white or color) each pixel would require different number of bits to represent the value of a pixel. The size of an image depends upon the number of pixels (also called resolution) and the bit pattern used to indicate the value of each pixel. Example: if an image is purely black and white (two color) each pixel can be represented by a value either 0 or 1, so an image made up of 10 x 10 pixel elements would require only 100 bits in memory to be stored. On the other hand an image that includes gray may require 2 bits to represent every pixel value (00 - black, 01 – dark gray, 10 – light gray, 11 –white). So the same 10 x 10 pixel image would now require 200 bits of memory to be stored. Commonly used Image formats : jpg, png, bmp, etc
4. Audio Data can also be in the form of sound which can be recorded and broadcasted. Example: What we hear on the radio is a source of data or information. Audio data is continuous, not discrete.
5. Video:-Video refers to broadcasting of data in form of picture or movie.

DATA FLOW

Two devices communicate with each other by sending and receiving data. The data can flow between the two devices in the following ways.

1. Simplex
2. Half Duplex
3. Full Duplex

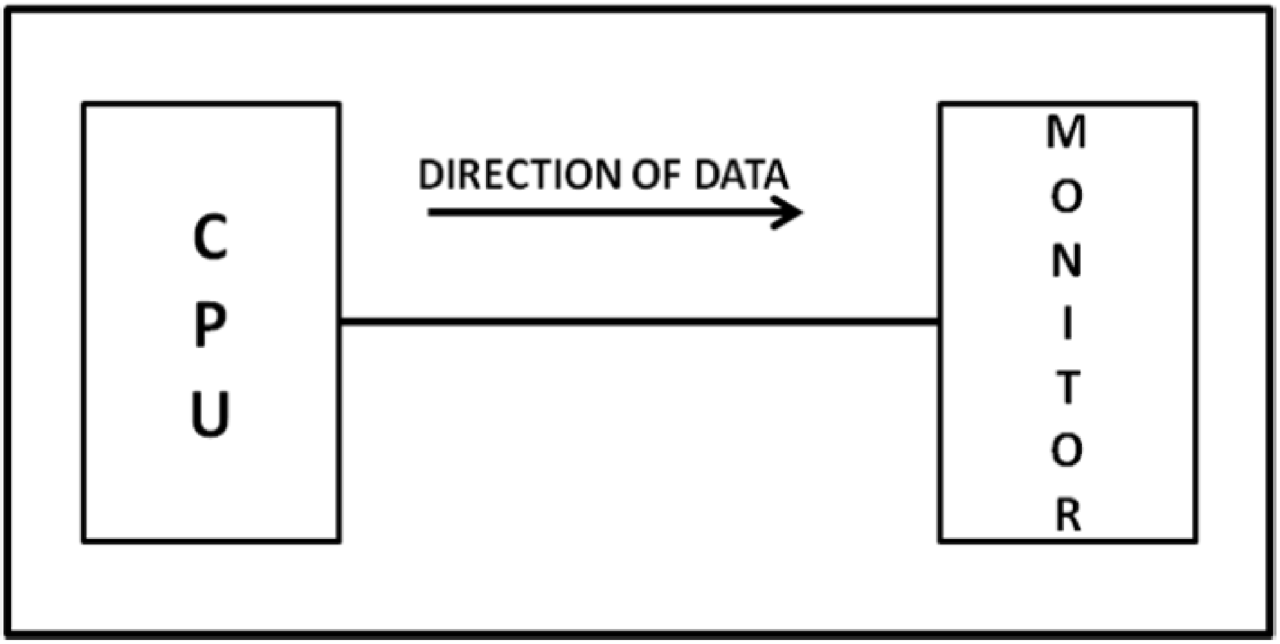


Figure: Simplex mode of communication

Fig 1.2

In Simplex, communication is unidirectional. Only one of the devices sends the data and the other one only receives the data. Example: in the above diagram: a cpu send data while a monitor only receives data.

Half Duplex

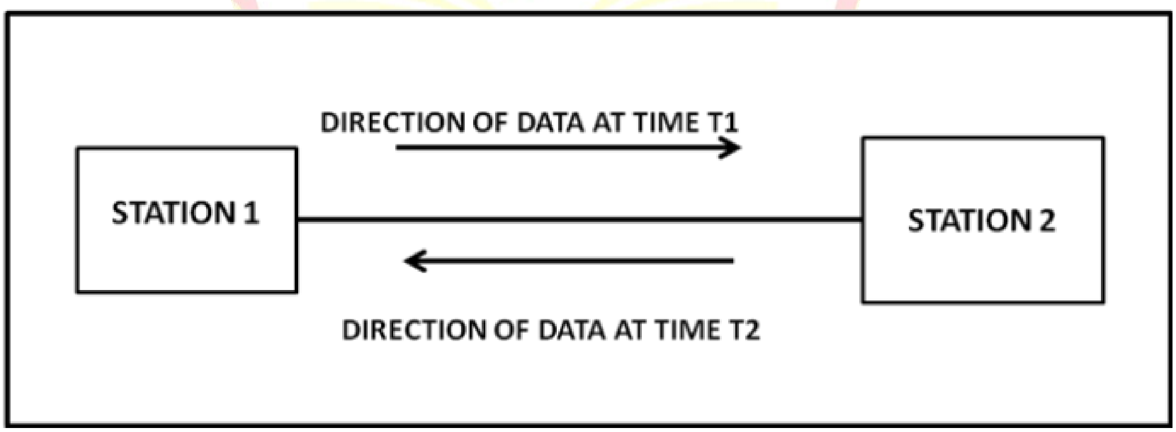


Figure: Half Duplex Mode of Communication

Fig 1.3

In half duplex, both the stations can transmit as well as receive but not at the same time. When one device is sending other can only receive and vice-versa (as shown in figure above.) Example: A walkie-talkie.

Full Duplex

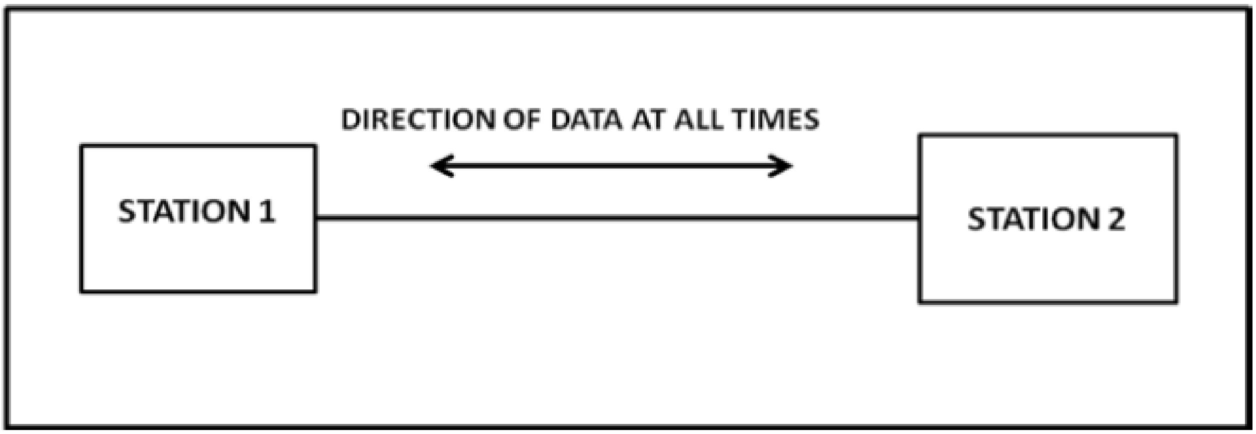


Figure: Full Duplex Mode of Communication

Fig 1.4

In Full duplex mode, both stations can transmit and receive at the same time. Example: mobile phones

DATA & SIGNALS

To be transmitted, data must be transformed to electromagnetic signals.

Data can be Analog or Digital.

1. Analog data refers to information that is continuous; ex. sounds made by a human voice
2. Digital data refers to information that has discrete states. Digital data take on discrete values.

For example, data are stored in computer memory in the form of Os and 1s

Signals can be of two types:
1. Analog Signal: They have infinite values in a range.
2. Digital Signal: They have limited number of defined values

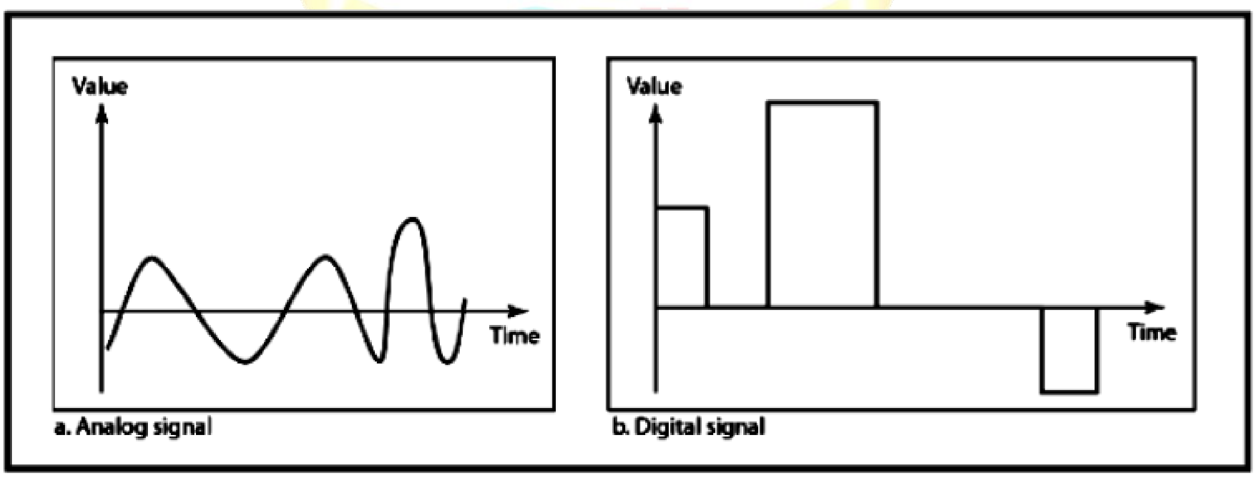


Fig 1.5

Signals which repeat itself after a fixed time period are called Periodic Signals. Signals which do not repeat itself after a fixed time period are called Non-Periodic Signals.

In data communications, we commonly use periodic analog signals and non-periodic digital signals.

ANALOG SIGNAL

An analog signal has infinitely many levels of intensity over a period of time.

As the wave moves from value A to value B, it passes through and includes an infinite number of values along its path as it can be seen in the figure below.

A simple analog signal is a sine wave that cannot be further decomposed into simpler signals.

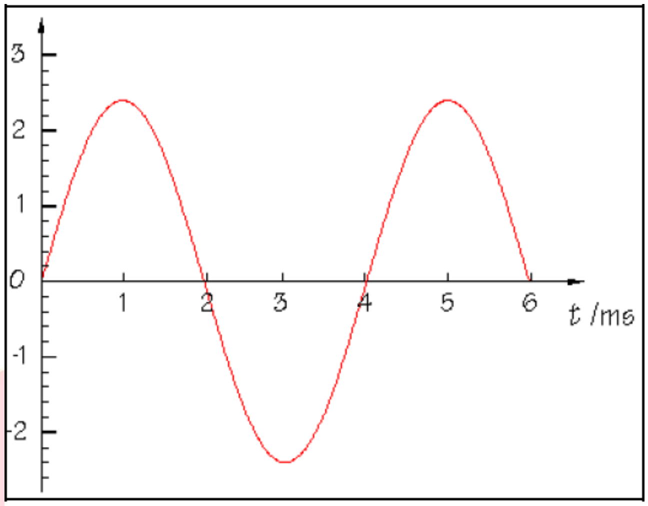


Fig. Sine wave

Fig 1.5

A sine wave is characterized by three parameters:

1. Peak Amplitude
2. Frequency
3. Phase

Characteristics of an Analog Signal

Peak Amplitude: The amplitude of a signal is the absolute value of its intensity at time t. The peak amplitude of a signal is the absolute value of the highest intensity. The amplitude of a signal is proportional to the energy carried by the signal.

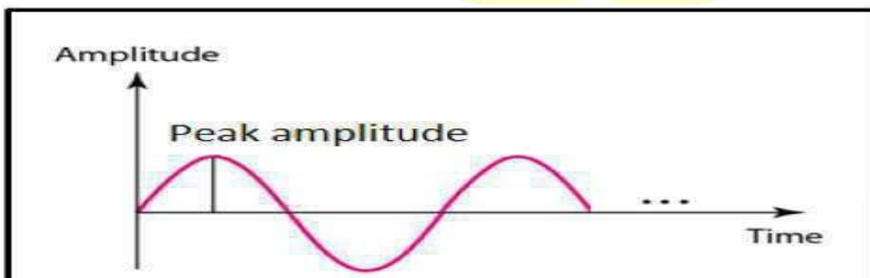


Fig.
Signal with high peak amplitude

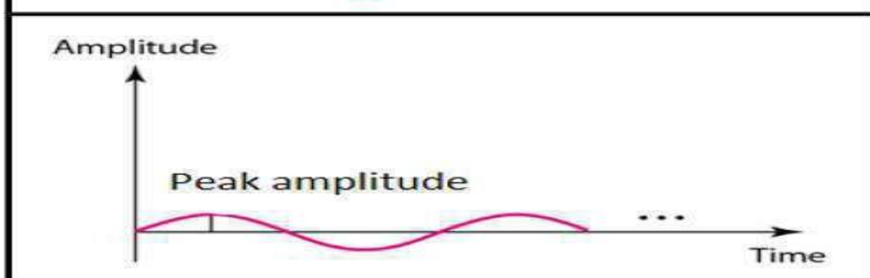


Fig.
Signal with low peak amplitude

Fig 1.6

Frequency

Frequency refers to the number of cycles completed by the wave in one second. Period refers to the time taken by the wave to complete one second.

Phase describes the position of the waveform with respect to time (specifically relative to time O).

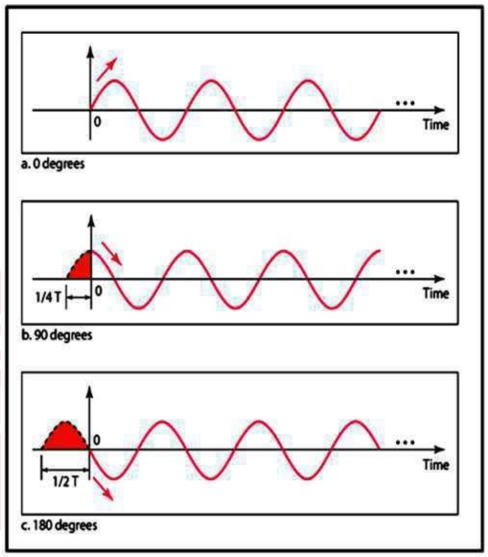


Fig: Phase of a sine wave

Fig 1.8

Phase indicates the forward or backward shift of the waveform from the axis. It is measured in degrees or radian. The figure above shows the sine waves with same amplitude and frequency but different phases

Digital Signal

Information can also be explained in the form of a digital signal. A digital signal can be explained with the help of following points:

1. A digital is a signal that has discrete values.
2. The signal will have value that is not continuous.

LEVEL

1. Information in a digital signal can be represented in the form of voltage levels.
2. Ex. In the signal shown below, a '1' is represented by a positive voltage and a '0' is represented by a Zero voltage.

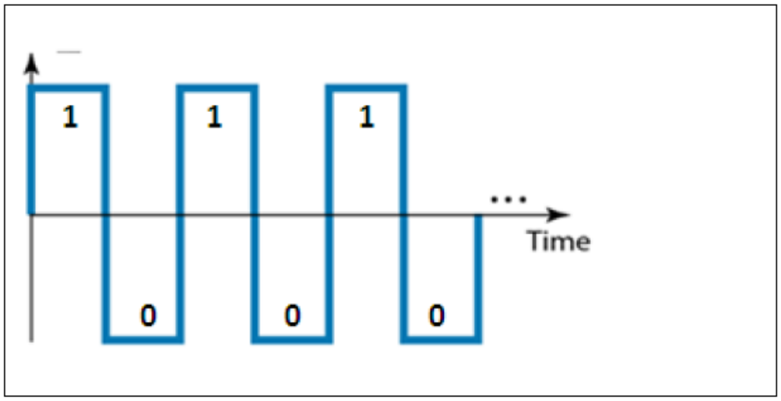


Fig: A digital signal with Two levels. '1' represented by a positive voltage and '0' represented by a negative voltage

- A Signal can have more than two levels

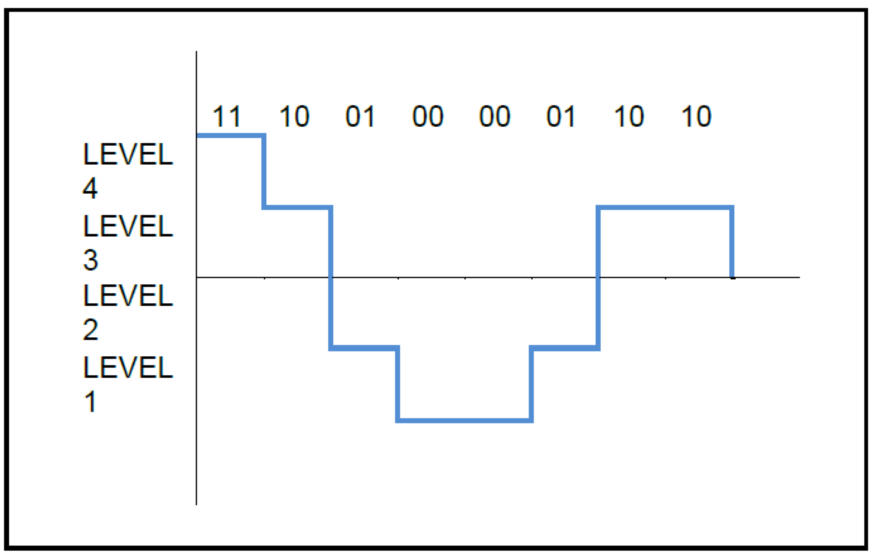
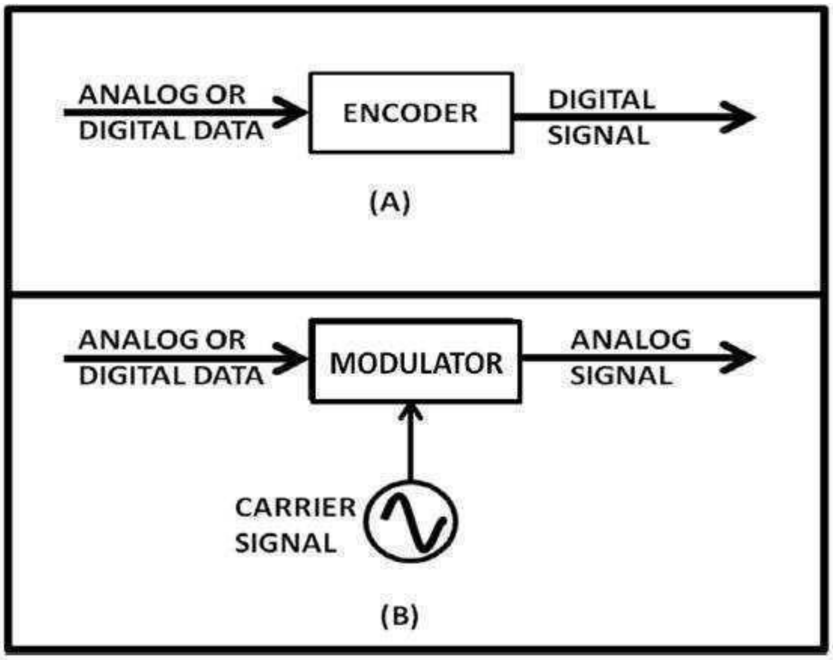


Fig: A digital signal with four levels

Fig 1.9

INTRODUCTION TO SIGNAL ENCODING

Data can be analog or digital, so can be the signal that represents it.Signal encoding is the conversion from analog/digital data to analog / digital



signal.

Figure: Signal Encoding

Fig 1.10

In the Figure above,

A) Demonstrates Digital Signaling where data from an analog/digital source is encoded into Digital Signal.

B) Demonstrates Analog signaling in which the analog/digital source modulates a continuous carrier signal to produce an analog signal.

The possible encodings are:

1. Digital data to Digital Signal
2. Digital data to Analog Signal
3. Analog data to Digital Signal
4. Analog data to Analog Signal

Digital Data to Digital Signal

Coding methods: Coding methods are used to convert digital data into digital signals.

There are two types of coding methods:

1 Line Coding

2 Block Coding

Scrambling is also one of the ways to convert digital data to digital signals but is not used.

Line Encoding

It is the process of converting Digital data into digital signal.

In other words, it is converting of binary data(i.e. A sequence of bits) into digital signal (i.e. a sequence of discrete, discontinuous voltage pulses)

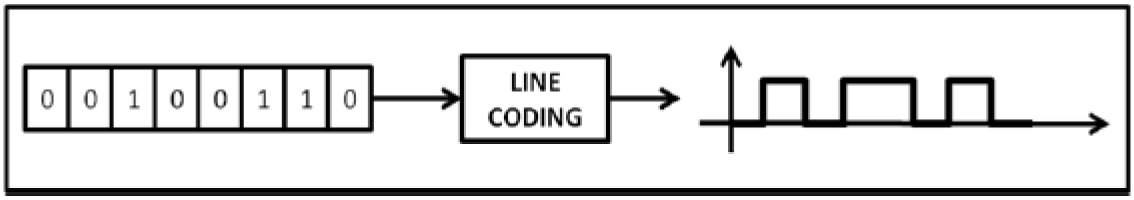


Figure: Line Coding

Fig 1.11

Classification of Line Codes

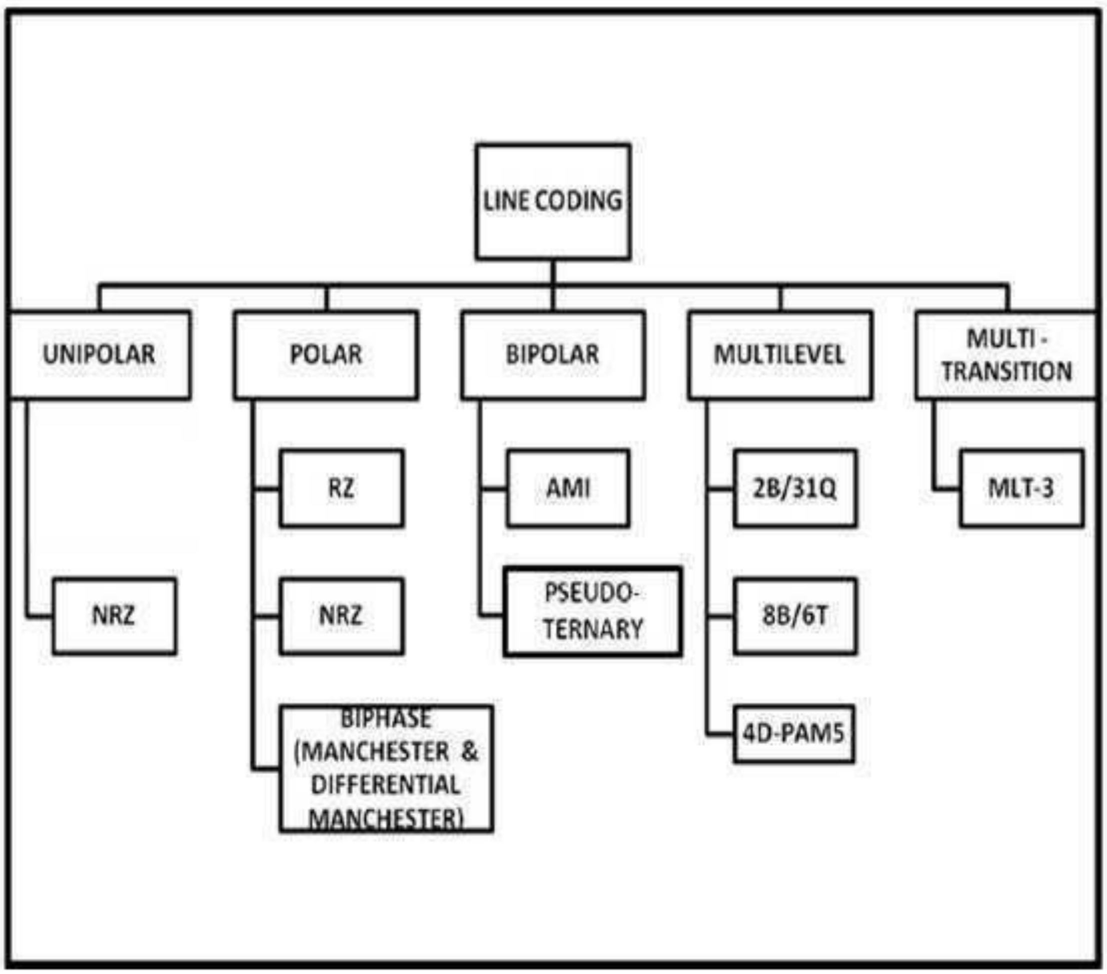


Figure : Classification of line coding schemes

Fig 1.12

Unipolar

All signal levels are either above or below the time axis.

NRZ - Non Return to Zero scheme is an example of this code. The signal level does not return to zero during a symbol transmission.

B Polar

NRZ-voltages are on both sides of the time axis.

Polar NRZ scheme can be implemented with two voltages. E.g. +V for 1 and -V for 0.

There are two variations:

NZR - Level (NRZ-L) - positive voltage for one symbol and negative for the other

NRZ - Inversion (NRZ-I) - the change or lack of change in polarity determines the value of a symbol. E.g. a "1" symbol inverts the polarity a "0" does not.

Polar – RZ - The Return to Zero (RZ) scheme uses three voltage values. +, 0, -.

Each symbol has a transition in the middle. Either from high to zero or from low to zero.

More complex as it uses three voltage level. It has no error detection capability

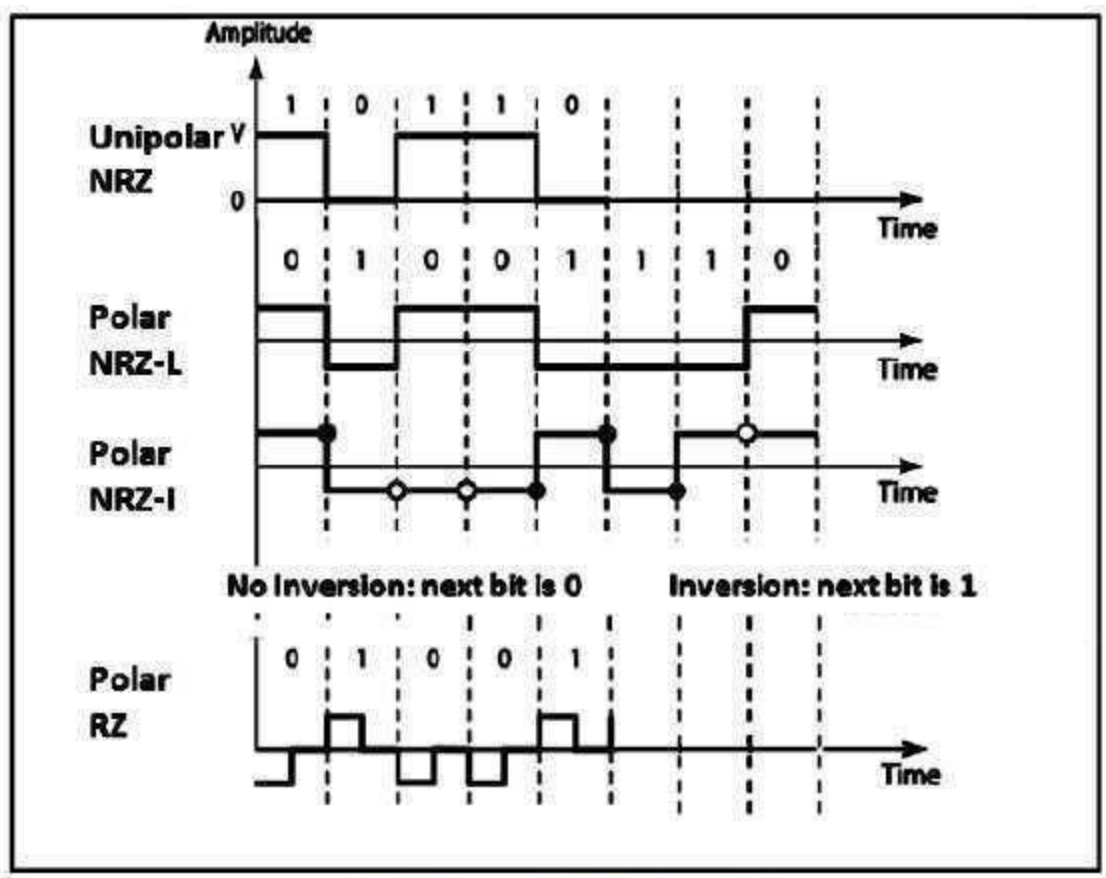


Figure : Unipolar(NRZ) & Polar(RZ & NRZ) Encoding

Fig 1.13

Polar - Biphase: Manchester and Differential Manchester

Manchester coding is a combination of NRZ-L and RZ schemes. Every symbol has a level transition in the middle: from high to low or low to high. It uses only two voltage levels.

Differential Manchester coding consists of combining the NRZ-I and RZ schemes. Every symbol has a level transition in the middle. But the level at the beginning of the symbol is determined by the symbol value. One symbol causes a level change the other does not.

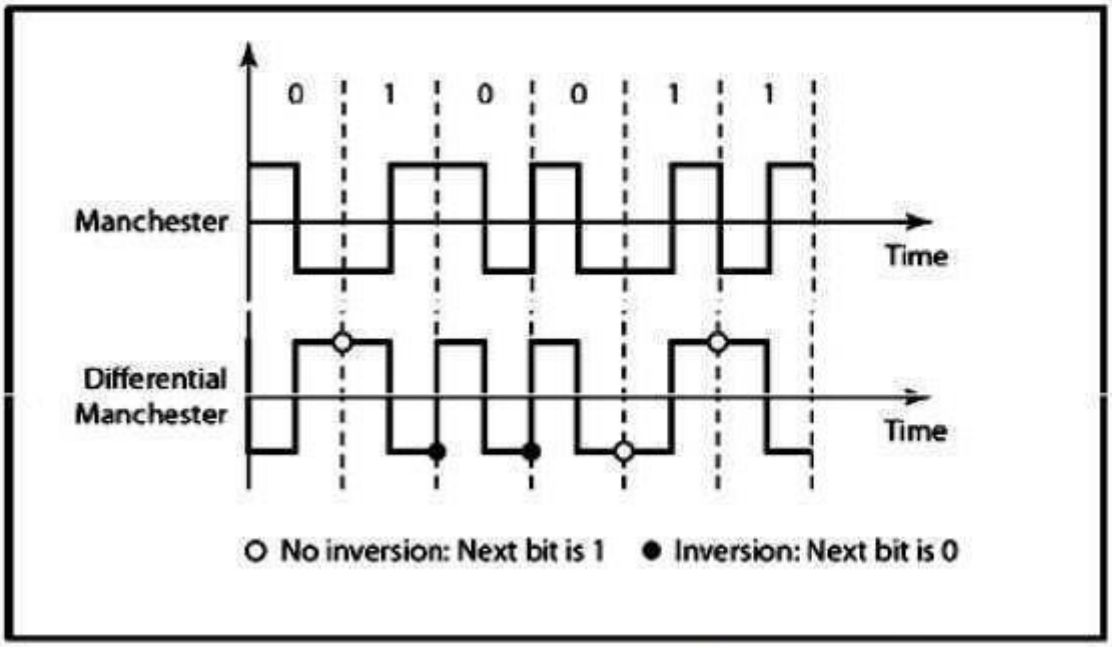


Figure : Polar biphase: Manchester and differential Manchester coding schemes

Fig 1.14

Bipolar - AMI and Pseudoternary

This coding scheme uses 3 voltage levels: - +, 0, -, to represent the symbols Voltage level for one symbol is at "0" and the other alternates between + & -.

Bipolar Alternate Mark Inversion (AMI) - the "0" symbol is represented by zero voltage and the "1" symbol alternates between +V and -V. Pseudoternary is the reverse of AMI

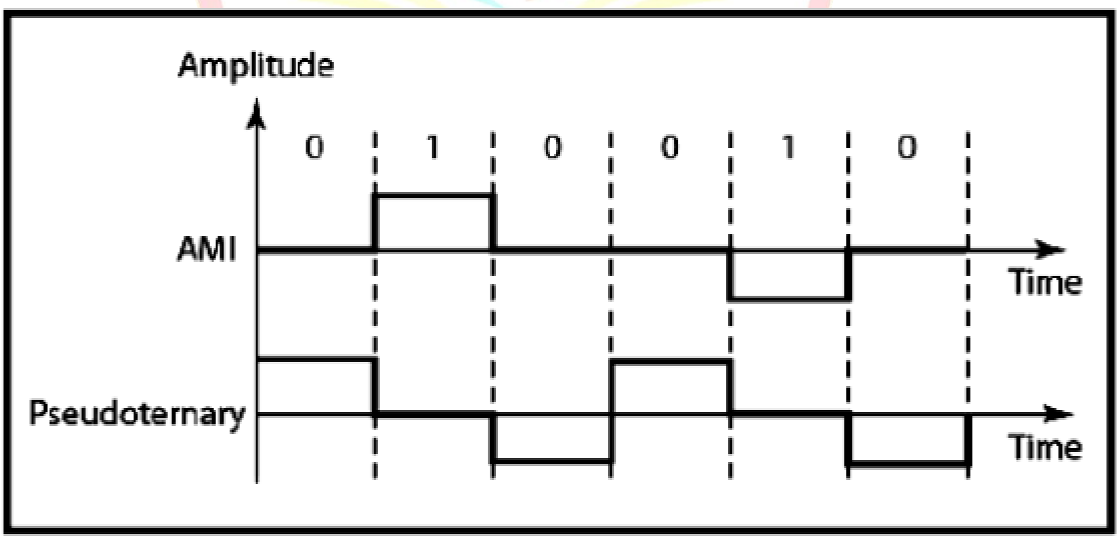


Figure: Bipolar coding scheme - AMI and Pseudoternary

Fig 1.15

Multilevel

Here the number of data bits is increased per symbol to increase the bit rate. 2 types of data element a 1 or a 0 are available, it can be combined into a pattern of n elements to create 2^m symbols. Using L signal levels we can have n signal elements to create L^n signal elements.

The following possibilities can occur: With 2^m symbols and L^n signals: If $2^m > L^n$ then we cannot represent the data elements, we don't have enough signals. If $2^m = L^n$ then we have an exact mapping of one symbol on one signal.
If $2^m < L^n$ then we have more signals than symbols and we can choose the signals that are more distinct to represent the symbols and therefore have better noise immunity and error detection as some signals are not valid These types of codings are classified as mBnL schemes.
In mBnL schemes, a pattern of m data elements is encoded as a pattern of n signal elements in which $2^m \leq L^n$. 2B1Q (two binary, one quaternary) Here m = 2; n = 1 ; Q = 4. It uses data patterns of size 2 and encodes the 2-bit patterns as one signal element belonging to a four-level signal.

	Positive level	Negative level
Next Bits	Next Level	Next Level
00	+1	-1
01	+3	-3
10	-1	+1
11	-3	+3

Transition Table

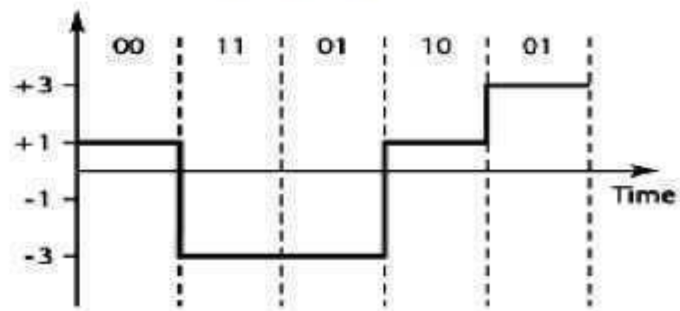


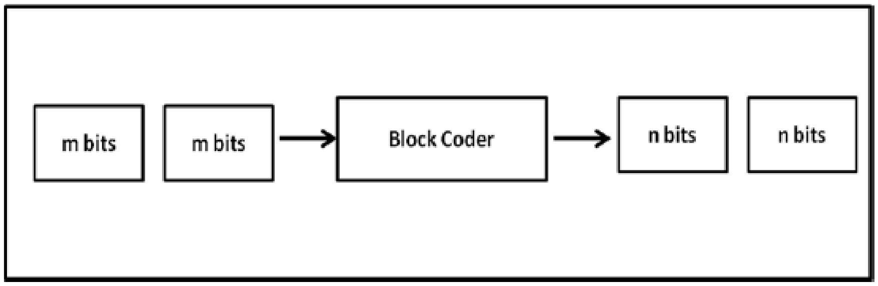
Figure: Multilevel coding scheme : 2B1Q

Fig 1.16

Block Coding

Block coding adds redundancy to line coding so that error detection can be implemented. Block coding changes a block of m bits into a block of n bits, where n is larger than m.

Block coding is referred to as an mB/nB encoding technique. The additional bits added to the original m bits‖ are called parity bits or check bits



m : message bits
Figure : Block Coding

Fig 1.17

Example: 4B/5B encoding Here a 4 bit code is converted into a 5 bit code.

TRANSMISSION MODES

Data is transmitted between two digital devices on the network in the form of bits. Transmission mode refers to the mode used for transmitting the data. The transmission medium may be capable of sending only a single bit in unit time or multiple bits in unit time.

When a single bit is transmitted in unit time the transmission mode used is Serial Transmission and when multiple bits are sent in unit time the transmission mode used is called Parallel transmission.

Types of Transmission Modes:

There are two basic types of transmission modes Serial and Parallel as shown in the figure below.
Serial transmission is further categorized into Synchronous and Asynchronous Serial transmission.

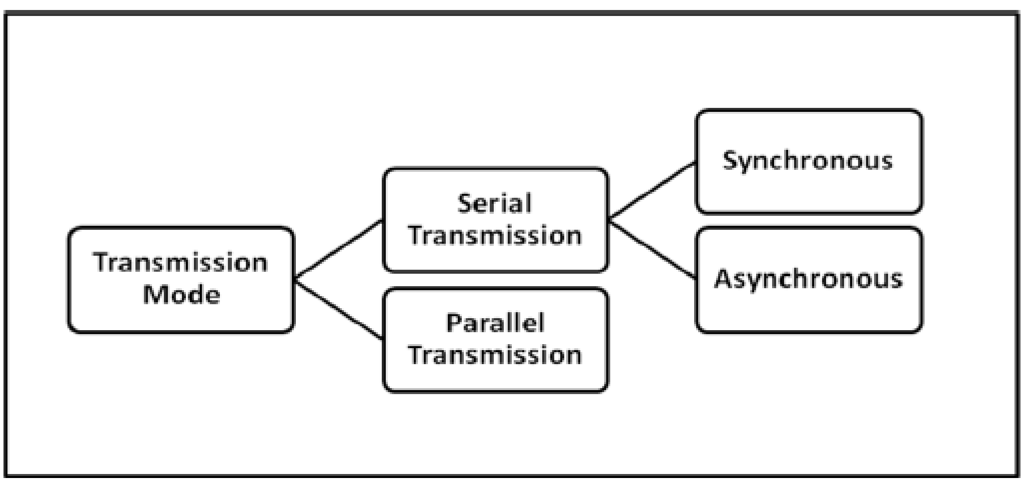


Fig. Types of Transmission Modes

Fig 1.18

Parallel Transmission

It involves simultaneous transmission of N bits over N different channels Parallel Transmission increases transmission speed by a factor of N over serial transmission.

Disadvantage of parallel transmission is the cost involved, N channels have to be used, hence, it can be used for short distance communication only.

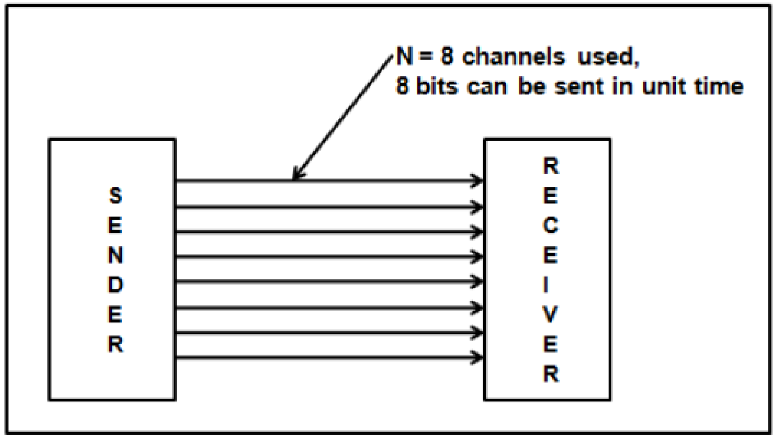


Fig. Parallel Transmission of Data over N = 8 channels

Fig 1.19

Example of Parallel Transmission is the communication between CPU and the Projector.

Serial Transmission

In Serial Transmission, as the name suggests data is transmitted serially, i.e. bit by bit, one bit at a time. Since only one bit has to be sent in unit time only a single channel is required.

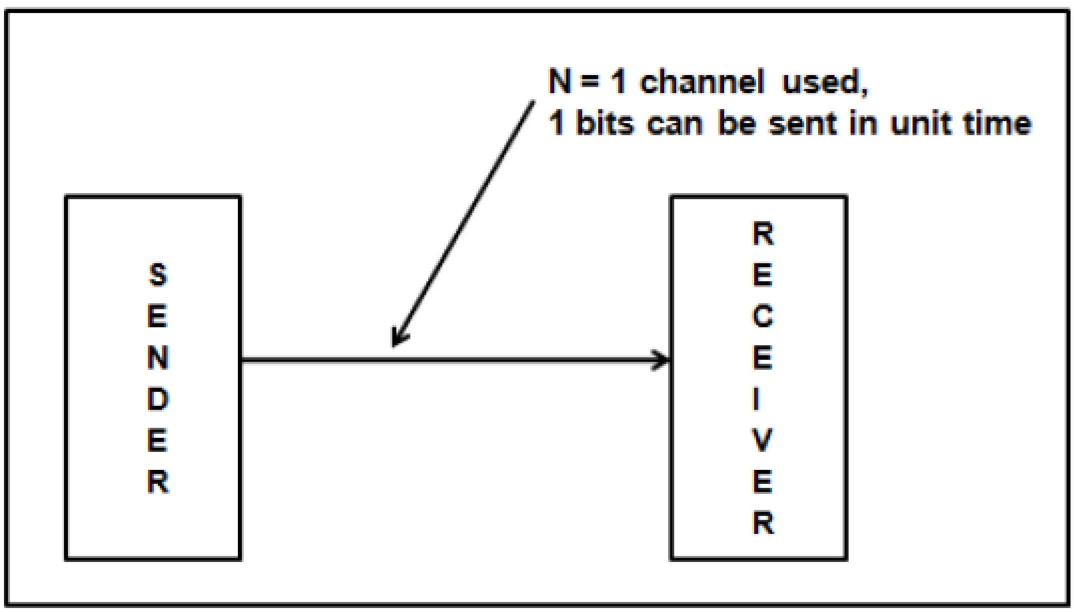


Fig. Serial Transmission of Data over N = 8 channels

Fig 1.20

Types of Serial Transmission: Depending upon the timing of transmission of data there are two types of serial transmission as described below:

ASynchronous Transmission

In asynchronous serial transmission the sender and receiver are not synchronized. The data is sent in group of 8 bits i.e. in bytes. The sender can start data transmission at any time instant without informing the receiver. To avoid confusing the receiver while receiving the data, ”start” and “stop” bits are inserted before and after every group of 8 bits as shown below.

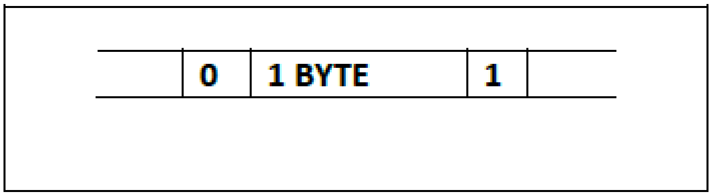


Fig: Start and Bit before and after every data byte

Fig 1.21

The start bit is indicated by "0" and stop bit is indicated by "1". The sender and receiver may not be synchronized as seen above but at the bit level they have to be synchronized i.e. the duration of one bit needs to be same for both sender and receiver for accurate data transmission. There may be gaps in between the data transmission indication that there is no data being transmitted from sender.

Ex. Assume a user typing at uneven speeds, at times there is no data being transmitted from Keyboard to the CPU. Following is the Diagram for Asynchronous Serial Transmission.

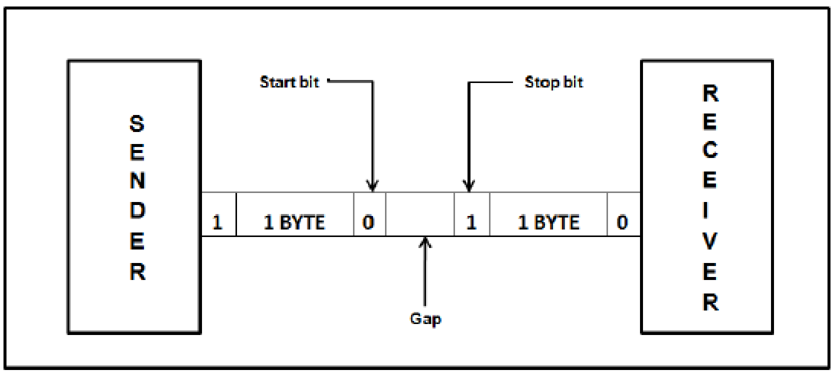


Fig: Asynchronous Serial Transmission

Fig 1.22

Advantages

1. Cheap and Effective implementation
2. Can be used for low speed communication Disadvantages Insertion of start bits, stop bits and gaps make asynchronous transmission slow. Application Keyboard

Synchronous Transmission: In Synchronous Serial Transmission, the sender and receiver are highly synchronized. No start, stop bits are used. Instead a common master clock is used for reference. The sender simply send stream of data bits in group of 8 bits to the receiver without any start or stop bit. It is the responsibility of the receiver to regroup the bits into units of 8 bits once they are received. When no data is being transmitted a sequence of 0's and 1's indicating IDLE is put on the transmission medium by the sender.

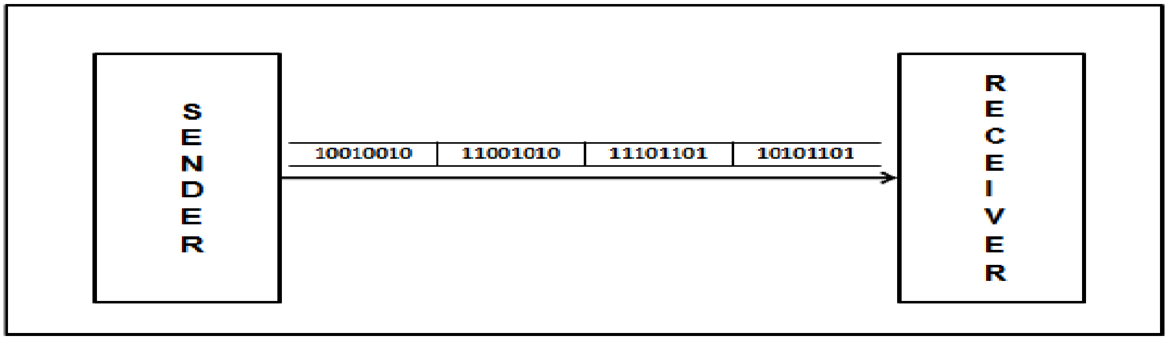


Fig: Asynchronous Serial Transmission

Fig 1.23

Advantage

1. There are no start bits, stop bits or gaps between data units
2. Since the above are absent data transmission is faster.
3. Due to synchronization there are no timing errors.

Sr.no	Parameter	Parallel transmission	Serial transmission
1	Number of wire required to transmit N bits	N wire	1 wire
2	Number of bits transmitted simultaneously	N bits	1 bit
3	Speed of data transfer	False	Slow
4	Cost	Higher due to more number of conductor	Low, since only one wire is used
5	Application	Short distance communication such as computer to printer communication	Long distance computer to computer communication.

Fig 1.24

Data Compression

Decreases space, time to transmit, and cost

• Bit rate is limited, can we send fewer bits and still deliver the data reliably? (‘educe the number of bits while retaining its meaning)
• Various approaches for data compression: Huffman, ‘un Length, LZW.

Huffman code
• Variable length code based on the frequency of character use.
– Most frequently used characters -> shortest codes
– Least frequently used characters -> longest codes
• A simple example – Text – EEEEAEEBFEEE (ASCII 12 * 7 = 84 bits)
E-0, A-100, B-101, F-110
Code – 000010000101110000 (18 bits)

Huffman code: Code formation
-Assign weights to each character
-Merge two lightest weights into one root node with sum of weights (why binary tree?)
-Repeat until one tree is left
-Traverse the tree from root to the leaf (for each node, assign 0 to the left, 1 to the right).

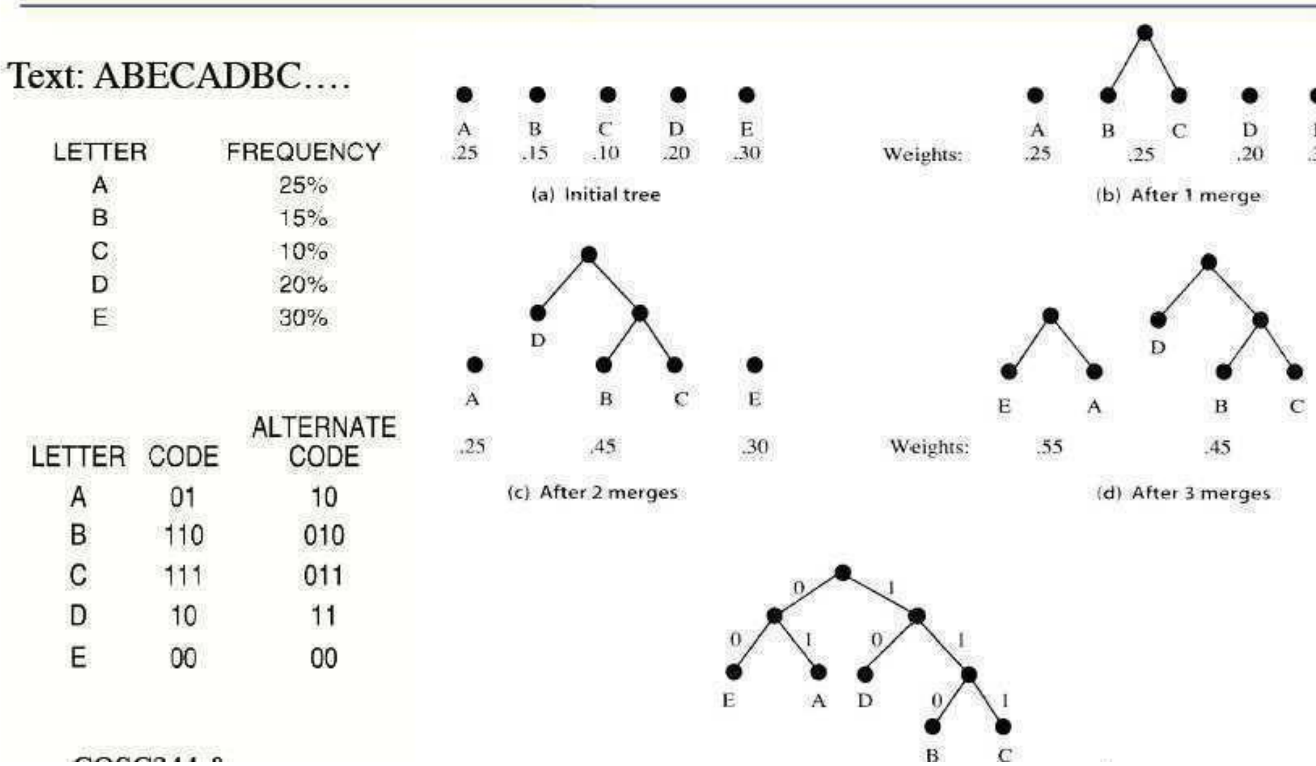


Fig 1.25

Huffman code: Code Interpretation
– No prefix property (Restriction): The code for any character never appears as the prefix or start of the code for any other character. (guarantees the codes can be translated back)
– Receiver continues to receive bits until it finds a code and forms the character – 01110001110110110111 (extract the string)
To each character, associate a binary tree consisting of just one node. To each tree, assign the character’ s frequency, which is called the tree’s weight.

ook for the two lightest-weight trees. If there are more than two, choose among them randomly. Merge the two into a single tree with a new root node whose left and right sub trees are the two we chose. Assign the sum of weights of the merged trees as the weight of the new tree.
-Repeat the previous step until just one tree is left.

Run Length Encoding (Character-Level)

Used for character data only

• Send an alternating set of numbers and characters.

• Example – HHHHHHHUFFFFFFFFFFFFFF – 7H1U14F

Run Length Encoding (Bit-Level)

1. Consider a picture of the letter T.
2. 70-90% of the space is white space, which means many continuous zeroes to be transmitted.
3. Group the runs of zeroes and send their length instead.
4. Decide the number of bits to represent a run length.

Encoding algorithm (4 bit lengths) – Count the number of 0s between two 1s

1. If the number is less than 15, write it down in binary form.
2. If it is greater than or equal to 15, write down 1111, and a following binary number to indicate the rest of the 0s. If more than 30, repeat this process.
3. If the data starts with a 1, write down 0000 at the beginning.
4. If the data ends with a 1, write down 0000 at the end.
5. Send the binary string.

Decoding algorithm

1. Group all the bits into 4-bit groups.
2. For each 4-bit group, write down that number of 0s.
3. If at the end of the bit string, stop.
4. If not at the end of the bit string: If the 4-bit group was less than 15, write down a 1. Go to step 1.
5. If the 4-bit group is 15, go to step 1.

Lempel-Ziv Compression

In text, phrases or entire words are repeated very often.

1. Look for repeated strings.
2. Store them and a code in a dictionary.
3. In the output, replace these repeated strings with the code.
4. zip, unzip, compress command in Unix.

UNIT-II

1.1 MULTIPLEXING

In telecommunications and computer networks, multiplexing (sometimes contracted to muxing) is a method by which multiple analog or digital signals are combined into one signal over a shared medium. The aim is to share a scarce resource. For example, in telecommunications, several telephone calls may be carried using one wire. Multiplexing originated in telegraphy in the 1870s, and is now widely applied in communications. In telephony, George Owen Squier is credited with the development of telephone carrier multiplexing in 1910.

The multiplexed signal is transmitted over a communication channel such as a cable. The multiplexing divides the capacity of the communication channel into several logical channels, one for each message signal or data stream to be transferred. A reverse process, known as demultiplexing, extracts the original channels on the receiver end.

A device that performs the multiplexing is called a multiplexer (MUX), and a device that performs the reverse process is called a demultiplexer (DEMUX or DMX).

Inverse multiplexing (IMUX) has the opposite aim as multiplexing, namely to break one data stream into several streams, transfer them simultaneously over several communication channels, and recreate the original data stream.

The set of techniques that allows the simultaneous transmission of multiple signals across a single data link.

1. Frequency-Division Multiplexing (FDM)
2. Wavelength-Division Multiplexing (WDM)
3. Time-Division Multiplexing (TDM)
4. Code-Division Multiplexing (CDM)

2.1a Frequency-Division Multiplexing Division Multiplexing (FDM)

• Each logical channel is transmitted on a separate frequency.
• Television and radio uses FDM to broadcast many channels over the same media.
• Filters separate the multiplexed signal back into its constituent component signals

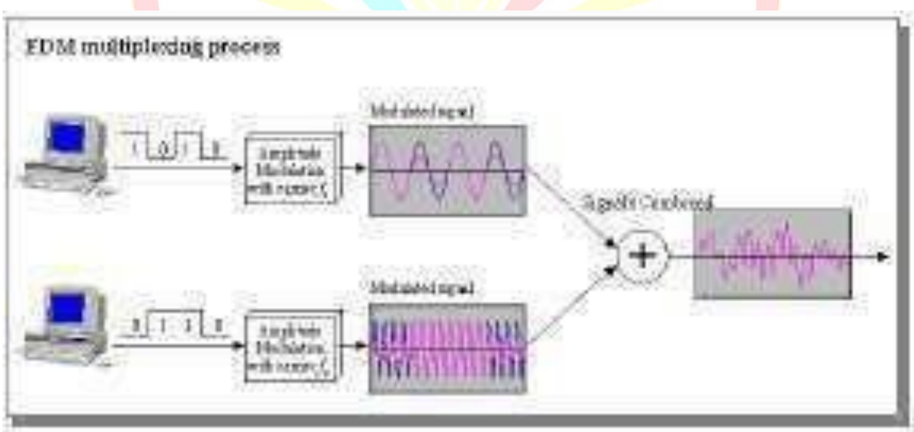


Fig 2.1a

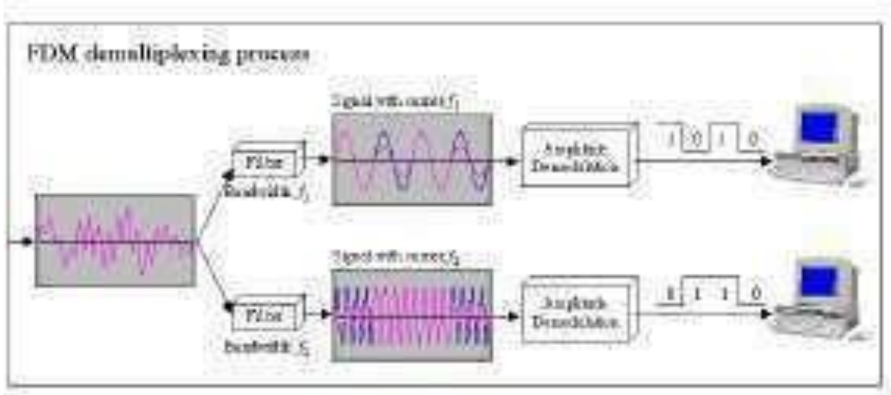


Fig 2.1b

2.1b Wavelength Division Multiplexing

• Theoretically identical to Frequency Division Multiplexing.
• Used in optical systems while FDM is used in electrical systems.
• Requires more spacing between channels

In fiber-optic communications, wavelength-division multiplexing (WDM) is a technology which multiplexes a number of optical carrier signals onto a single optical fiber by using different wavelengths (i.e., colors) of laser light. This technique enables bidirectional communications over one strand of fiber, as well as multiplication of capacity.

The term wavelength-division multiplexing is commonly applied to an optical carrier, which is typically described by its wavelength, whereas frequency-division multiplexing typically applies to a radio carrier which is more often described by frequency. This is purely convention because wavelength and frequency communicate the same information.

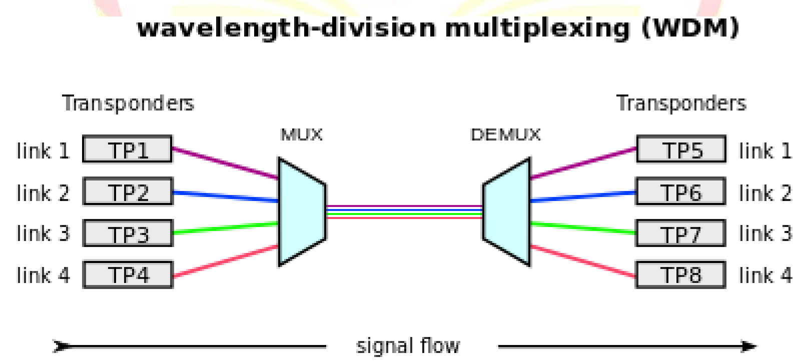


Fig 2.2

2.1c Time-Division Multiplexing Division Multiplexing (TDM)

• multiple transmissions can occupy a single link by subdividing them and interleaving the portions
• We refer to TDM as a "round robin" use of a frequency
• TDM can be implemented in two ways: 1. Synchronous TDM 2. Asynchronous TDM

2.1c.a Synchronous TDM

The multiplexer allocates exactly the same time slot to each device at all times, whether or not a device has anything to transmit

• A frame consists of one complete cycle of time slots. Thus the number of slots in frame is equal to the number of inputs.

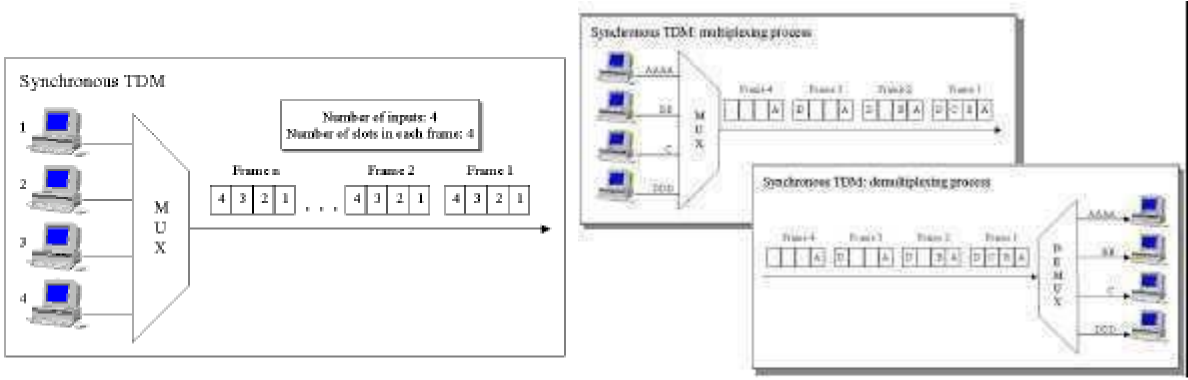


Fig 2.3

2.1 c.b Asynchronous TDM (or statistical time (or statistical time-division multiplexing)

Each slot in a frame is not dedicated to the fix device

• The number of slots in a frame is not necessary to be equal to the number of input devices. More than one slots in a frame can be allocated for an input device. Asynchronous TDM (or statistical time (or statistical time-division multiplexing) division multiplexing)

• Allows maximum utilization of the link. It allows a number of lower speed input lines to be multiplexed to a single higher speed line

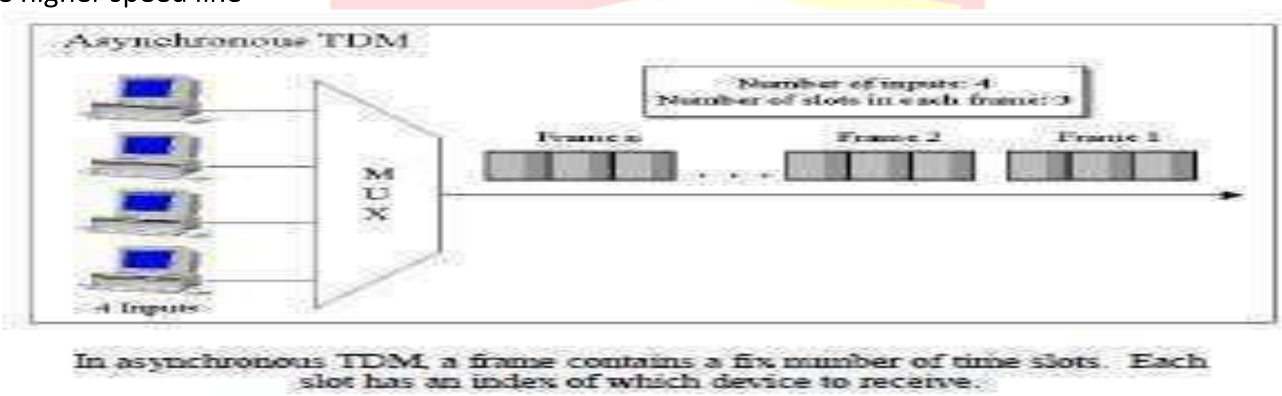


Fig 2.4

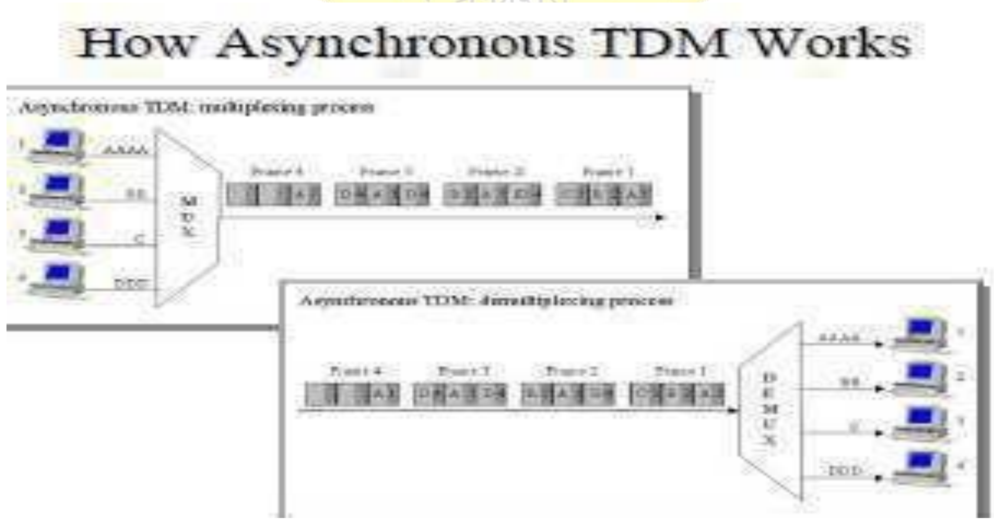


Fig 2.5

Code Division Multiplexing

• Sends many signals or “chips” per bit.
• Each sender uses a unique pattern of chips.
• May use multiple frequencies for spread spectrum communication.
• Common with wireless systems.

2.2 NORTH AMERICAN DIGITAL TELEPHONE HIERARCHY

To take advantage of merits of TDM and digital transmission, the common carriers employ a hierarchy of multiplexing.

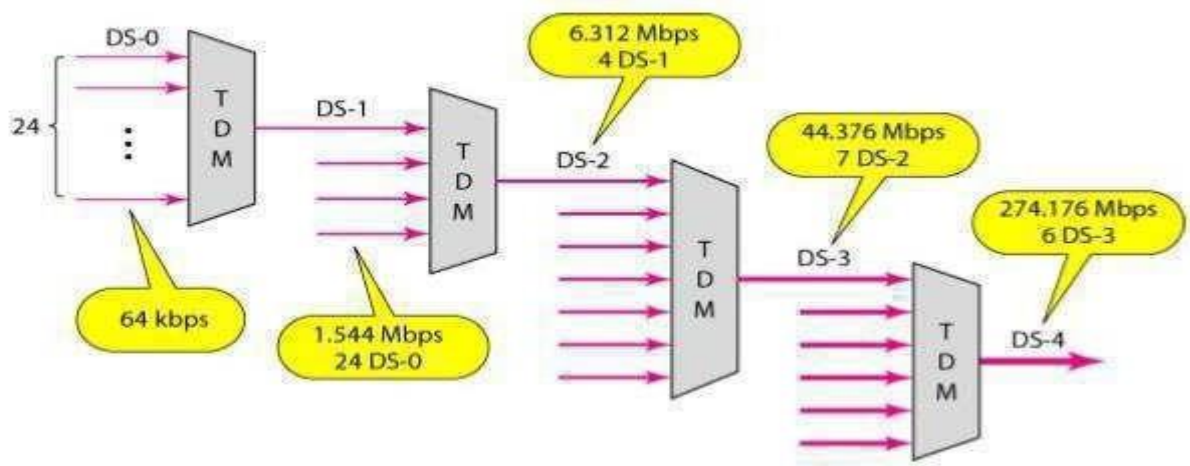


Fig 2.6

T1 Carrier System

T1 carrier systems were designed to combine PCM and TDM Techniques for the transmission of 24 64Kbps channels with each channel Capable of Carrying Digitally encoded voice band telephone signals or data. The transmission bit rate (line speed) for a T1 carrier is 1.544 Mbps.

All 24 DS-0 channels combined has a data rate of 1.544Mbps, this digital signal level is called DS-1. Therefore T1 lines are referred as DS-1 lines.

Service	Line	Rate (Mbps)	Voice Channels
DS-1	T-1	1.544	24
DS-2	T-2	6.312	96
DS-3	T-3	44.736	672
DS-4	T-4	274.176	4032

Fig 2.7

T2 Carrier System

T2 carriers time division multiplex 96 64-Kbps voice or data channels into a single 6.312 Mbps data signal for transmission over twisted pair copper wire upto 500 miles over a special metallic cable.

T3 Carrier system

T3 carriers Time division multiplex 672 64-kbps voice or data channels for transmission over a single coaxial cable. The transmission rate is 44.736 Mbps.

T4 Carrier System
T4 carriers time division multiplex 4032 64-kbps voice or data channels for transmitting over a single T4 coaxial cable upto 500 mile. The transmission rate is very high i.e. 274.16Kbps.

T5 Carrier System
T5 carriers time division multiplex 8064 64Kbps voice or data channels and transmit them at 560.16Mbps over a single coaxial cable.

2.3 EUROPEAN TDM
The E-carrier is a member of the series of carrier systems developed for digital transmission of many simultaneous telephone calls by time-division multiplexing. The European Conference of Postal and Telecommunications Administrations (CEPT) originally standardized the E-carrier system, which revised and improved the earlier American T-carrier technology, and this has now been adopted by the International Telecommunication Union Telecommunication Standardization Sector (ITU-T). It was widely adopted in almost all countries outside the US, Canada, and Japan. E-carrier deployments have steadily been replaced by Ethernet as telecommunication networks transitions towards all IP.

E1 frame structure
An E1 link operates over two separate sets of wires, usually Unshielded twisted pair (balanced cable) or using coaxial (unbalanced cable). A nominal 3 volt peak signal is encoded with pulses using a method avoiding long periods without polarity changes. The line data rate is 2.048 Mbit/s (full duplex, i.e. 2.048 Mbit/s downstream and 2.048 Mbit/s upstream) which is split into 32 timeslots, each being allocated 8 bits in turn. Thus each timeslot sends and receives an 8-bit PCM sample, usually encoded according to A-law algorithm, 8,000 times per second ($8 \times 8{,}000 \times 32 = 2{,}048{,}000$). This is ideal for voice telephone calls where the voice is sampled at that data rate and reconstructed at the other end. The timeslots are numbered from 0 to 31.

Frame alignment

In an E1 channel, communication consists of sending consecutive frames from the transmitter to the receiver. The receiver must receive an indication showing when the first interval of each frame begins, so that, since it knows to which channel the information in each time slot corresponds, it can demultiplex correctly. This way, the bytes received in each slot are assigned to the correct channel. A synchronization process is then established, and it is known as frame alignment.The E1 frame defines a cyclical set of 32 time slots of 8 bits. The time slot 0 is devoted to transmission management and time slot 16 for signaling; the rest were assigned originally for voice/data transport.

Frame-alignment signal

In order to implement the frame alignment system so that the receiver of the frame can tell where it begins, there is so called a frame alignment signal (FAS). In the 2 Mbit/s frame system, the FAS is a combination of seven fixed bits ("0011011") transmitted in the first time slot in the frame (time slot zero or TS0). For the alignment mechanism to be maintained, the FAS does not need to be transmitted in every frame. Instead, this signal can be sent in alternate frames (in the first, in the third, in the fifth, and so on). In this case, TS0 is used as the synchronization slot. The TS0 of the rest of the frames is therefore available for other functions, such as the transmission of the alarms.

Special timeslots
One timeslot (TS0) is reserved for framing purposes, and alternately transmits a fixed pattern. This allows the receiver to lock onto the start of each frame and match up each channel in turn. The standards allow for a full

cyclic redundancy check to be performed across all bits transmitted in each frame, to detect if the circuit is losing bits (information), but this is not always used. An alarm signal may also be transmitted using timeslot TS0. Finally, some bits are reserved for national use.
One timeslot (TS16) is often reserved for signalling purposes, to control call setup and teardown according to one of several standard telecommunications protocols. This includes channel-associated signaling (CAS) where a set of bits is used to replicate opening and closing the circuit (as if picking up the telephone receiver and pulsing digits on a rotary phone), or using tone signalling which is passed through on the voice circuits themselves. More recent systems use common-channel signaling (CCS) such Signalling System 7 (SS7) where no timeslot is reserved for signalling purposes, the signalling protocol being transmitted on a different physical channel.

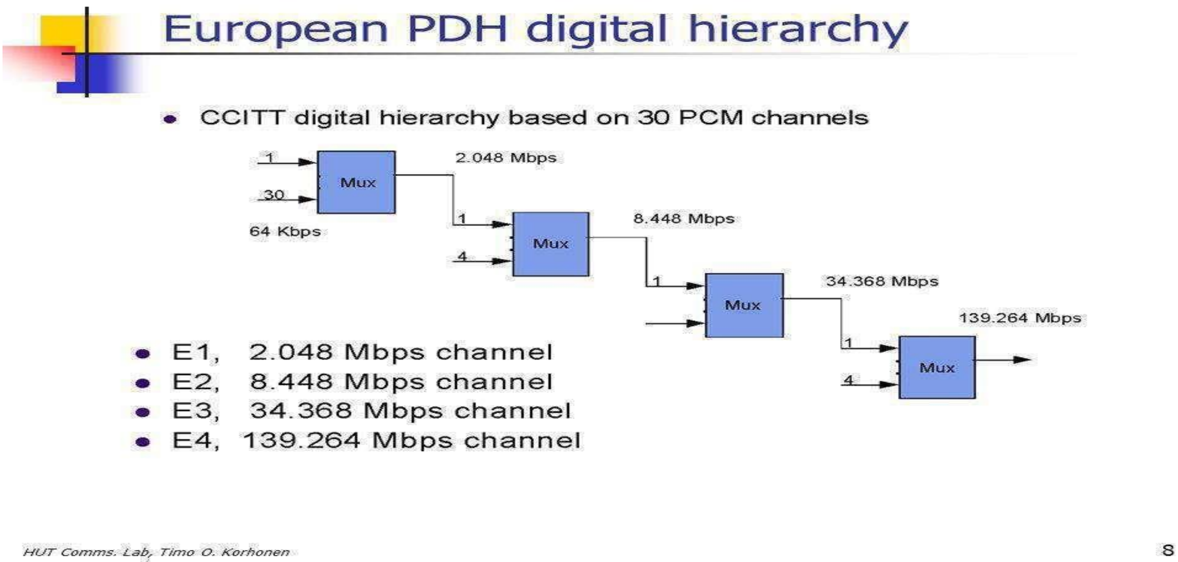


Fig 2.8

2.4 SPREAD SPECTRUM

spread-spectrum techniques are methods by which a signal (e.g., an electrical, electromagnetic, or acoustic signal) generated with a particular bandwidth is deliberately spread in the frequency domain, resulting in a signal with a wider bandwidth. These techniques are used for a variety of reasons, including the establishment of secure communications, increasing resistance to natural interference, noise and jamming, to prevent detection, and to limit power flux density.
This is a technique in which a telecommunication signal is transmitted on a bandwidth considerably larger than the frequency content of the original information. Frequency hopping is a basic modulation technique used in spread spectrum signal transmission.
Spread-spectrum telecommunications is a signal structuring technique that employs direct sequence, frequency hopping, or a hybrid of these, which can be used for multiple access and/or multiple functions. This technique decreases the potential interference to other receivers while achieving privacy. Spread spectrum generally makes use of a sequential noise-like signal structure to spread the normally narrowband information signal over a relatively wideband (radio) band of frequencies. The receiver correlates the received signals to retrieve the original information signal. Originally there were two motivations: either to resist enemy efforts to jam the communications (anti-jam, or AJ), or to hide the fact that communication was even taking place, sometimes called low probability of intercept (LPI), low probability of detection.

Frequency-hopping spread spectrum (FHSS), direct-sequence spread spectrum (DSSS), time-hopping spread spectrum (THSS), chirp spread spectrum (CSS), and combinations of these techniques are forms of spread spectrum. Each of these techniques employs pseudorandom number sequences—created using pseudorandom number generators—to determine and control the spreading pattern of the signal across the allocated bandwidth. Wireless standard IEEE 802.11 uses either FHSS or DSSS in its radio interface.

2.4a Direct-sequence spread spectrum

In telecommunications, direct-sequence spread spectrum (DSSS) is a spread spectrum modulation technique used to reduce overall signal interference. The spreading of this signal makes the resulting wideband channel more noisy, allowing for greater resistance to unintentional and intentional interference.

A method of achieving the spreading of a given signal is provided by the modulation scheme. With DSSS, the message signal is used to modulate a bit sequence known as a Pseudo Noise (PN) code; this PN code consists of a radio pulse that is much shorter in duration (larger bandwidth) than the original message signal. This modulation of the message signal scrambles and spreads the pieces of data, and thereby resulting in a bandwidth size nearly identical to that of the PN sequence. In this context, the duration of the radio pulse for the PN code is referred to as the chip duration. The smaller this duration, the larger the bandwidth of the resulting DSSS signal; more bandwidth multiplexed to the message signal results in better resistance against interference.

Some practical and effective uses of DSSS include the Code Division Multiple Access (CDMA) channel access method and the IEEE 802.11b specification used in Wi-Fi networks.

Direct-sequence spread-spectrum transmissions multiply the data being transmitted by a "noise" signal. This noise signal is a pseudorandom sequence of 1 and −1 values; at a frequency much higher than that of the original signal.

The resulting signal resembles white noise, like an audio recording of "static". However, this noise-like signal is used to exactly reconstruct the original data at the receiving end, by multiplying it by the same pseudorandom sequence (because $1 \times 1 = 1$, and $-1 \times -1 = 1$). This process, known as "de-spreading", mathematically constitutes a correlation of the transmitted PN sequence with the PN sequence that the receiver already knows the transmitter is using.

The resulting effect of enhancing signal to noise ratio on the channel is called process gain. This effect can be made larger by employing a longer PN sequence and more chips per bit, but physical devices used to generate the PN sequence impose practical limits on attainable processing gain.

While for useful process gain the transmitted DSSS signal must occupy much wider bandwidth than simple wave of the original signal alone would require, its frequency spectrum can be somewhat restricted for spectrum economy by a conventional analog bandpass filter to give a roughly bell-shaped envelope centered on the carrier frequency. In contrast, frequency-hopping spread spectrum which pseudo-randomly re-tunes the carrier, instead of adding pseudo-random noise to the data, requires a uniform frequency response since any bandwidth shaping would cause amplitude modulation of the signal by the hopping code.

If an undesired transmitter transmits on the same channel but with a different PN sequence (or no sequence at all), the de-spreading process has reduced processing gain for that signal. This effect is the basis for the code division multiple access (CDMA) property of DSSS, which allows multiple transmitters to share the same channel within the limits of the cross-correlation properties of their PN sequences.

DSSS-Direct Sequence Spread Spectrum

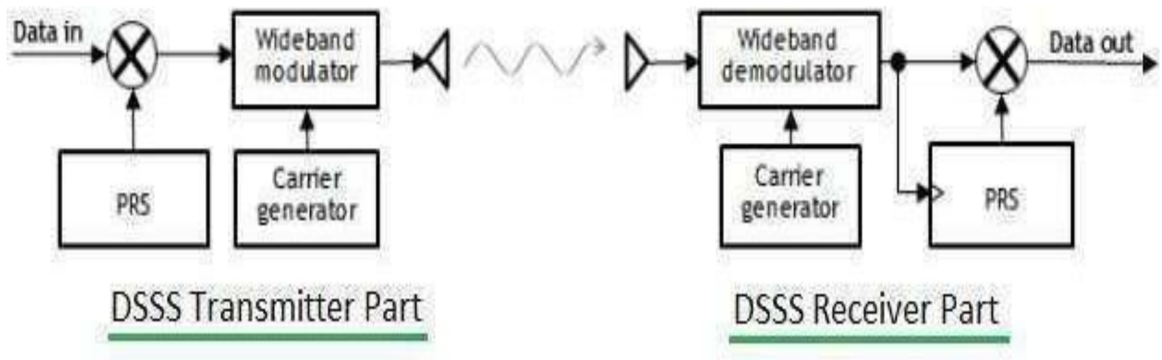


Fig 2.9

In **DSSS**, which stands for Direct Sequence Spread Spectrum, information bits are modulated by PN codes(chips). PN codes are Pseudonoise code symbols. This PN codes have short duration compare to information bits. Here transmitted information over the air occupies more bandwidth compare to user informaion bits. DSSS is the modulation technique adopted in IEEE 802.11 based WLAN compliant products. In DSSS systems entire system bandwidth is available for each user all the time.

The figure drawn above depicts DSSS Transmitter and DSSS receiver Block Diagram. PRS stands for Pseudo-Random Sequence.

2.4 b FHSS-Frequency Hopping Spread Spectrum

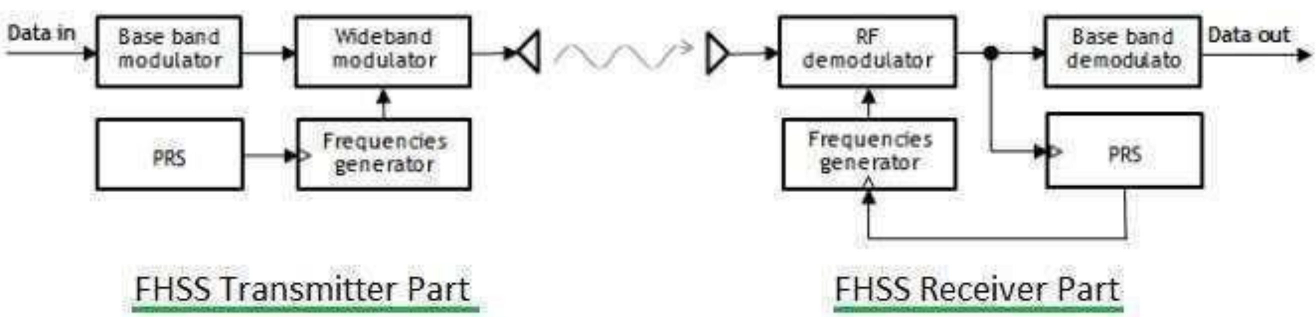


Fig 2.10

In **FHSS**, which stands for Frequency Hopping Spread Spectrum, RF carrier frequency is changed according to the Pseudo-random sequence(PRS or PN sequence). This PN sequence is known to both transmitter and Receiver and hence help demodulate/decode the information. Within one chip duration, RF frequency does not vary. Based on this fact there are two types of FHSS, fast hopped FHSS and slow hopped FHSS.

In Fast hopped FHSS, hopping is done at the rate faster than message(information) bit rate. In slow hopped FHSS, hopping is done at the rate slower than information bit rate.

The figure2.7 drawn above depicts FHSS Transmitter and DSSS receiver Block Diagram.

Difference between DSSS and FHSS

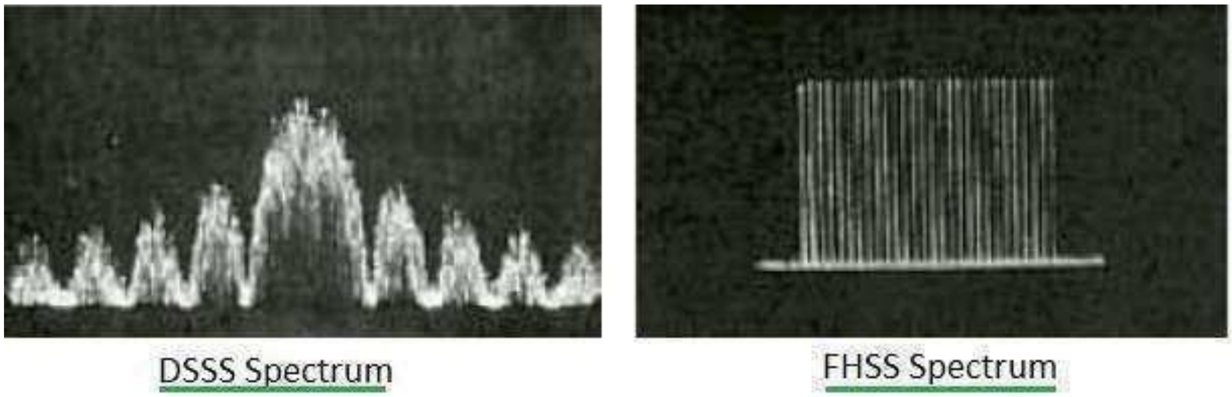


Fig 2.11

This figure 2.11depicts DSSS spectrum and FHSS spectrum.

• As FHSS systems rely on varying RF carrier frequency, it leads to bursty nature of errors due to frequency selective fading mainly. For more information on different types of channel models rayleigh, rician fading refer to page on channel model by William Stallings.

• In DSSS, information bits are spread across both frequency and time planes, hence minimizes effect of interference as well as fading. Hence DSSS system prone to errors but at low level compare to FHSS systems. FHSS produces strong bursty errors.

• DSSS delivers capacity upto 11 Mbps while FHSS supports upto 3 Mbps.

• DSSS is very sensitive technology while FHSS is very robust technology. This is observed in harsh environment comprising large coverage, noises, collocated cells, multi-path and presence of bluetooth frequency waves etc.

DSSS is ideal for point to point applications while FHSS can be used in point to multipoint deployment with excellent performance.

Modem short for modulator-demodulator. In communication modem convert the digital data in to analog so that it transmit over the phone line because phone line transmit analog data. in the same way on the other hand when data is received modem again convert this analog data in to digital single so that computer store and process on this information.

2.5 TERMINAL HANDLING PRINCIPLES

• Terminal access to mainframe and mini computers used hardwired terminals typically connected through a RS232 serial line.
• Today the normal command line interface to FreeBSD use a pseudo terminal.
• A pseudo terminal is built from a device pair termed the master and slave devices.
• The master side is named /dev/ptyXX and the slave side is named /dev/ttyXX.
• The slave device provides to a process an interface identical to that historically provided by a hardware device.
• Anything written on a master device appears as input on the slave device and anything written on a slave appears as input on the master device.
• Pseudo terminals are used by the terminal emulator, xterm, and by remote login programs such as ssh.
• Xterm opens the master side of the pseudo terminal and directs the keystrokes to its output and input from the pseudo terminal is directed to the window.

• Xterm forks a child process that opens the slave side of the pseudo terminal and execs a user shell.

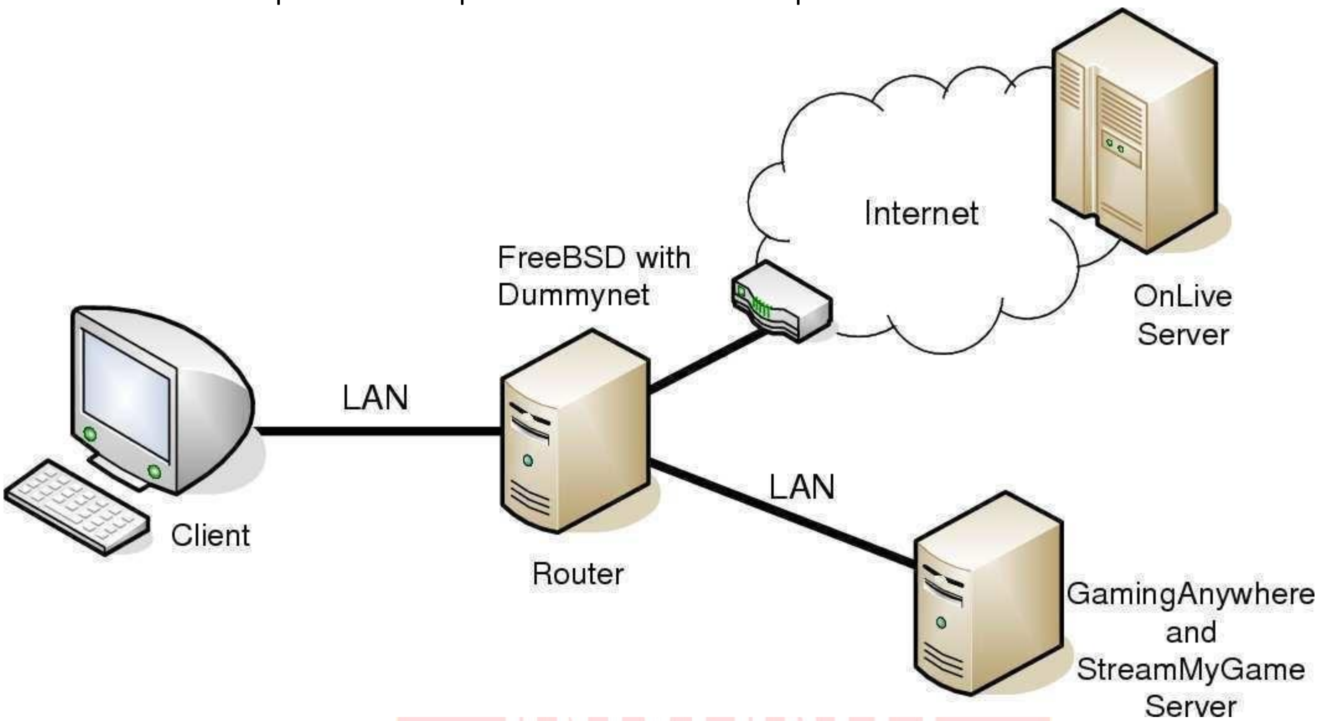


Fig. 2.12

Terminal Modes-The terminal processing can be set to two different modes, canonical mode (clocked mode) and noncanonical mode (raw mode).

Canonical mode properties:

• Characters are echoed by the operating system as they are typed but are buffered internally until a newline character ,NL, is typed.
• Only after a NL character is received the entire line is made available to the reading process.
• If the process tries to read before a NL character is received it is put to sleep until an NL character arrives.
• Typing errors can be corrected by entering special erase and kill characters.
• Simple output processing is performed - normally converting a NL character to NL + CR (carriage return).
• When a process has filled the terminal output queue it will be put to sleep.
• The system makes each typed character available to the reading process as soon as it is received.
• No line editing or other processing is performed. In reality many combinations of these modes can be specified.

2.6 POLLING

Polling is the process where the computer or controlling device waits for an external device to check for its readiness or state, often with low-level hardware. For example, when a printer is connected via a parallel port, the computer waits until the printer has received the next character. These processes can be as minute as only reading one bit. This is sometimes used synonymously with busy-wait polling. In this situation, when an I/O operation is required, the computer does nothing other than check the status of the I/O device until it is ready, at which point the device is accessed. In other words, the computer waits until the device is ready. Polling also refers to the situation where a device is repeatedly checked for readiness, and if it is not, the computer returns to a different task. Although not as wasteful of CPU cycles as busy waiting, this is generally not as efficient as the alternative to polling, interrupt-driven I/O.

In a simple single-purpose system, even busy-wait is perfectly appropriate if no action is possible until the I/O access, but more often than not this was traditionally a consequence of simple hardware or non-multitasking operating systems.

Polling is often intimately involved with very low-level hardware. For example, polling a parallel printer port to check whether it is ready for another character involves examining as little as one bit of a byte. That bit represents, at the time of reading, whether a single wire in the printer cable is at low or high voltage. The I/O instruction that reads this byte directly transfers the voltage state of eight real world wires to the eight circuits (flip flops) that make up one byte of a CPU register. Polling has the disadvantage that if there are too many devices to check, the time required to poll them can exceed the time available to service the I/O device.

Algorithm

Polling can be described in the following steps :

1. The host repeatedly reads the busy bit of the controller until it becomes clear.
2. When clear, the host writes in the command register and writes a byte into the data-out register.
3. The host sets the command-ready bit (set to 1).
4. When the controller senses command-ready bit is set, it sets busy bit.
5. The controller reads the command register and since write bit is set, it performs necessary I/O operations on the device. If the read bit is set to one instead of write bit, data from device is loaded into data-in register, which is further read by the host.
6. The controller clears the command-ready bit once everything is over, it clears error bit to show successful operation and reset busy bit (0).

TYPES

A. A polling cycle is the time in which each element is monitored once. The optimal polling cycle will vary according to several factors, including the desired speed of response and the overhead (e.g., processor time and bandwidth) of the polling.
B. In roll call polling, the polling device or process queries each element on a list in a fixed sequence. Because it waits for a response from each element, a timing mechanism is necessary to prevent lock-ups caused by non-responding elements. Roll call polling can be inefficient if the overhead for the polling messages is high, there are numerous elements to be polled in each polling cycle and only a few elements are active.
C. In hub polling, also referred to as token polling, each element polls the next element in some fixed sequence. This continues until the first element is reached, at which time the polling cycle starts all over again.
D. Polling can be employed in various computing contexts in order to control the execution or transmission sequence of the elements involved. For example, in multitasking operating systems, polling can be used to allocate processor time and other resources to the various competing processes.
E. In networks, polling is used to determine which nodes want to access the network. It is also used by routing protocols to retrieve routing information, as is the case with EGP (exterior gateway protocol).
F. An alternative to polling is the use of interrupts, which are signals generated by devices or processes to indicate that they need attention, want to communicate, etc. Although polling can be very simple, in many situations (e.g., multitasking operating systems) it is more efficient to use interrupts because it can reduce processor usage and/or bandwidth consumption.

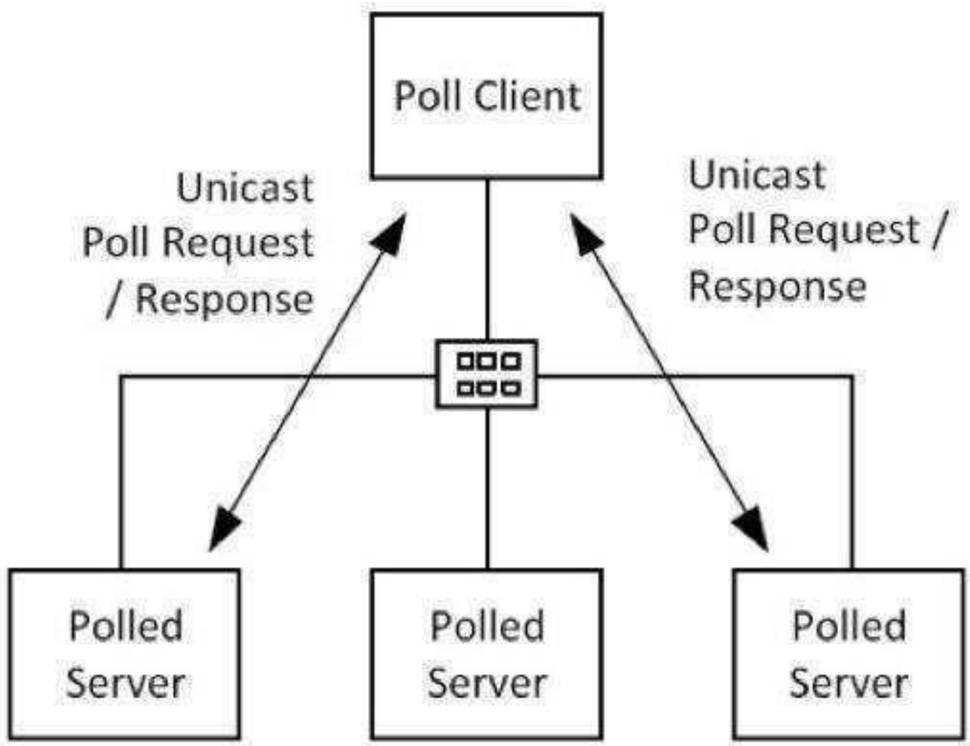


Fig. 2.13

2.7 SWITCHED COMMUNICATION NETWORK

Switching Techniques - In large networks there might be multiple paths linking sender and receiver. Information may be switched as it travels through various communication channels.

There are four typical switching techniques available for digital traffic.

1. Circuit Switching
2. Packet Switching
3. Message Switching
4. Cell Switching

2.7a Circuit Switching

1. Circuit switching is a technique that directly connects the sender and the receiver in an unbroken path.
2. Telephone switching equipment, for example, establishes a path that connects the caller's telephone to the receiver's telephone by making a physical connection.
3. With this type of switching technique, once a connection is established, a dedicated path exists between both ends until the connection is terminated.
4. Routing decisions must be made when the circuit is first established, but there are no decisions made after that time.
5. Circuit switching in a network operates almost the same way as the telephone system works.
6. A complete end-to-end path must exist before communication can take place.
7. The computer initiating the data transfer must ask for a connection to the destination.
8. Once the connection has been initiated and completed to the destination device, the destination device must acknowledge that it is ready and willing to carry on a transfer.
9. The communication channel (once established) is dedicated.

Disadvantages:

• Possible long wait to establish a connection, (10 seconds, more on long- distance or international calls.) during which no data can be transmitted.

• More expensive than any other switching techniques, because a dedicated path is required for each connection.
• Inefficient use of the communication channel, because the channel is not used when the connected systems are not using it.

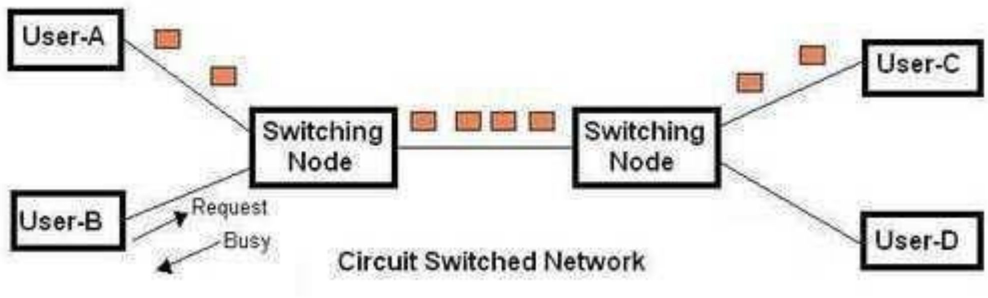


Fig 2.14

2.7b Packet Switching

Advantages:

* Packet switching can be seen as a solution that tries to combine the advantages of message and circuit switching and to minimize the disadvantages of both.
* There are two methods of packet switching: Datagram and virtual circuit.
* In both packet switching methods, a message is broken into small parts, called packets.
* Each packet is tagged with appropriate source and destination addresses.
* Since packets have a strictly defined maximum length, they can be stored in main memory instead of disk; therefore access delay and cost are minimized.
* Also the transmission speeds, between nodes, are optimized.
* With current technology, packets are generally accepted onto the network on a first-come, first-served basis. If the network becomes overloaded, packets are delayed or discarded (``dropped'').

The size of the packet can vary from 180 bits, the size for the Datakit virtual circuit switch designed by Bell Labs for communications and business applications; to 1,024 or 2,048 bits for the 1PSS switch, also designed by Bell Labs for public data networking; to 53 bytes for ATM switching, such as Lucent Technologies' packet switches.

* In packet switching, the analog signal from your phone is converted into a digital data stream. That series of digital bits is then divided into relatively tiny clusters of bits, called packets. Each packet has at its beginning the digital address -- a long number -- to which it is being sent. The system blasts out all those tiny packets, as fast as it can, and they travel across the nation's digital backbone systems to their destination: the telephone, or rather the telephone system, of the person you're calling.
* They do not necessarily travel together; they do not travel sequentially. They don't even all travel via the same route.But eventually they arrive at the right point -- that digital address added to the front of each string of digital data -- and at their destination are reassembled into the correct order, then converted to analog form, so your friend can understand what you're saying.
* Datagram packet switching is similar to message switching in that each packet is a self-contained unit with complete addressing information attached.
* This fact allows packets to take a variety of possible paths through the network.
* So the packets, each with the same destination address, do not follow the same route, and they may arrive out of sequence at the exit point node (or the destination).
* Reordering is done at the destination point based on the sequence number of the packets.
* It is possible for a packet to be destroyed if one of the nodes on its way is crashed momentarily. Thus all its queued packets may be lost.
* In the virtual circuit approach, a preplanned route is established before any data packets are sent.

* A logical connection is established when a sender send a "call request packet" to the receiver and the receiver send back an acknowledge packet "call accepted packet" to the sender if the receiver agrees on conversational parameters.
• The conversational parameters can be maximum packet sizes, path to be taken, and other variables necessary to establish and maintain the conversation.
• Virtual circuits imply acknowledgements, flow control, and error control, so virtual circuits are reliable. That is, they have the capability to inform upper-protocol layers if a transmission problem occurs
• In virtual circuit, the route between stations does not mean that this is a dedicated path, as in circuit switching.
* A packet is still buffered at each node and queued for output over a line.

The difference between virtual circuit and datagram approaches:
* With virtual circuit, the node does not need to make a routing decision for each packet.
* It is made only once for all packets using that virtual circuit. VC's offer guarantees that the packets sent arrive in the order sent with no duplicates or omissions with no errors (with high probability) regardless of how they are implemented internally.
Advantages:
• Packet switching is cost effective, because switching devices do not need massive amount of secondary storage.
• Packet switching offers improved delay characteristics, because there are no long messages in the queue (maximum packet size is fixed).
• Packet can be rerouted if there is any problem, such as, busy or disabled links.
* The advantage of packet switching is that many network users can share the same channel at the same time. Packet switching can maximize link efficiency by making optimal use of link bandwidth.
Disadvantages:
• Protocols for packet switching are typically more complex.
• It can add some initial costs in implementation.
• If packet is lost, sender needs to retransmit the data. Another disadvantage is that packet-switched systems still can't deliver the same quality as dedicated circuits in applications requiring very little delay - like voice conversations or moving images.

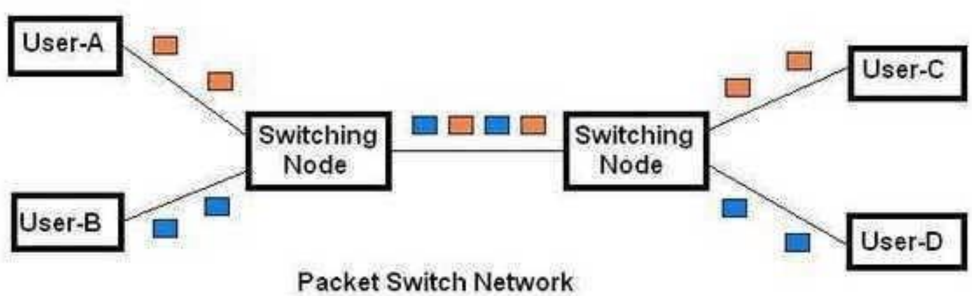


Fig 2.15

2.7c Message Switching:
• With message switching there is no need to establish a dedicated path between two stations.
• When a station sends a message, the destination address is appended to the message.
• The message is then transmitted through the network, in its entirety, from node to node.
• Each node receives the entire message, stores it in its entirety on disk, and then transmits the message to the next node.
• This type of network is called a store-and-forward network.

A message-switching node is typically a general-purpose computer. The device needs sufficient secondary-storage capacity to store the incoming messages, which could be long. A time delay is introduced using this type of scheme due to store- and-forward time, plus the time required to find the next node in the transmission path.

Advantages:

- Channel efficiency can be greater compared to circuit-switched systems, because more devices are sharing the channel.
- Traffic congestion can be reduced, because messages may be temporarily stored in route.
- Message priorities can be established due to store-and-forward technique.
- Message broadcasting can be achieved with the use of broadcast address appended in the message.

Disadvantages

- Message switching is not compatible with interactive applications.
- Store-and-forward devices are expensive, because they must have large disks to hold potentially long

Fig 2.16

Cell Switching

Cell Switching is similar to packet switching, except that the switching does not necessarily occur on packet boundaries. This is ideal for an integrated environment and is found within Cell-based networks, such as ATM. Cell-switching can handle both digital voice and data signals.

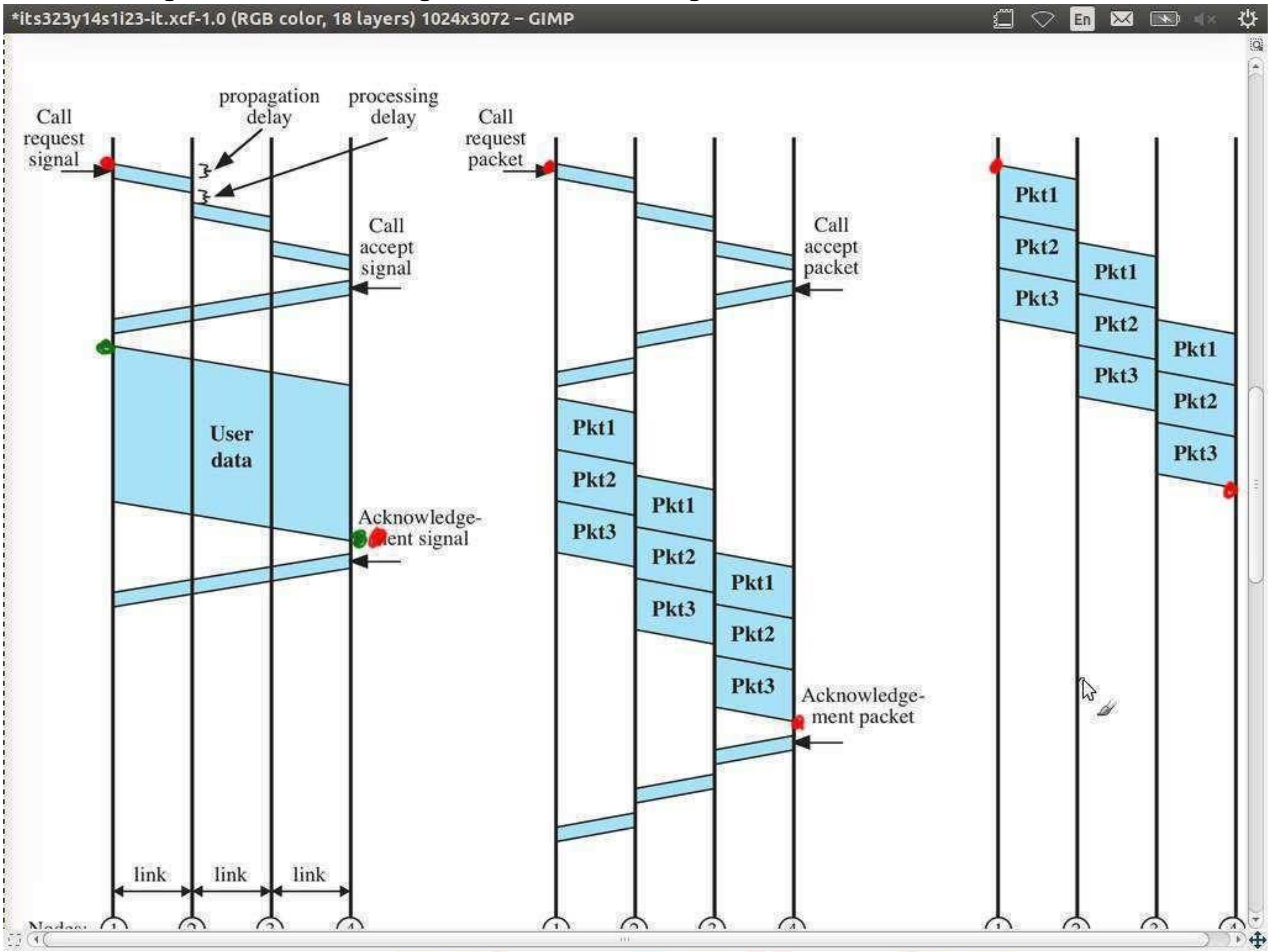


Fig 2.17

1.8 SOFT SWITCH ARCHITECTURE WITH THEIR COMPARATIVE STUDY

A softswitch (software switch) is a central device in a telecommunications network which connects telephone calls from one phone line to another, across a telecommunication network or the public Internet, entirely by means of software running on a general-purpose computer system. Most landline calls are routed by purpose-built electronic hardware; however, soft switches using general purpose servers and VoIP technology are becoming more popular.

Many telecommunications networks now make use of combinations of softswitches and more traditional purpose-built hardware.

Although the term softswitch technically refers to any such device, it is more conventionally applied to a device that handles IP-to-IP phone calls, while the phrase "access server" or "media gateway" is used to refer to devices that either originate or terminate traditional "land line" (hard wired) phone calls. In practice, such devices can often do both. As a practical distinction, a Skype-to-Skype phone call is entirely IP (internet) based, and so uses a softswitch somewhere in the middle connecting the calling party with the called party. In contrast, access servers might take a mobile call or a call originating from a traditional phone line, convert it to IP traffic, then send it over the internet to another such device, which terminates the call by reversing the

process and converting the Voice over IP call back to older circuit switched digital systems
digital ISDN / PSTN protocols that transmit voice traffic using non-IP systems.

A softswitch is typically used to control connections at the junction point between circuit-switched and packet-switched networks. A single device containing both the switching logic and the switched fabric can be used for this purpose; however, modern technology has led to a preference for decomposing this device into a Call Agent and a Media Gateway.

The Call Agent takes care of functions such as billing, call routing, signaling, call services and the like, supplying the functional logic to accomplish these telephony meta-tasks. A call agent may control several different media gateways in geographically dispersed areas via a TCP/IP link. It is also used to control the functions of media gateway, in order to connect with media as well as other interfaces. This procedure is utilized to keep the interfaces clear as crystal for receiving calls from any phone lines.

The media gateway connects different types of digital media stream together to create an end-to-end path for the media (voice and data) in the call. It may have interfaces to connect to traditional PSTN networks, such as DS1 or DS3 ports (E1 or STM1 in the case of non-US networks). It may also have interfaces to connect to ATM and IP networks, and the most modern systems will have Ethernet interfaces to connect VoIP calls. The call agent will instruct the media gateway to connect media streams between these interfaces to connect the call - all transparently to the end-users.

The softswitch generally resides in a building owned by the telephone company called a telephone exchange (UK/IRL/AUS/NZ) or central office (US/CAN). The central office or telephone exchange has high capacity connections to carry calls to other offices owned by the telecommunication company and to other telecommunication companies via the PSTN.

Looking towards the end users from the switch, the softswitch may be connected to several access devices via TCP/IP network. These access devices can range from small Analog Telephone Adaptors (ATA) which provide just one RJ11 telephone jack to an Integrated Access Device (IAD), eMTA s (embedded Multimedia Terminal Adapters) using MGCP/NCS protocol over cable (VoCable) or PBX which may provide several hundred telephone connections

Note here that Analogue (ATA), PSTN telephone devices can only be reached by a softswitch that has embedded SS7 or SIGTRAN cards, software in terms of signalling AND Trunking Gateway for Voice traffic IP/TDM, TDM/IP, TDM/TDM functions.

Typically the larger access devices will be located in a building owned by the telecommunication company near to the customers they serve. Each end user can be connected to the IAD by a simple pair of copper wires. The medium-sized devices and PBXs are most commonly used by business that locate them on their own premises, and single-line devices are mostly found at private residences.

At the turn of the 21st century with IP Multimedia Subsystem (or IMS), the Softswitch element is represented by the Media Gateway Controller (MGC) element, and the term "Softswitch" is rarely used in the IMS context. Rather, it is called an AGCF (Access Gateway Control Function).

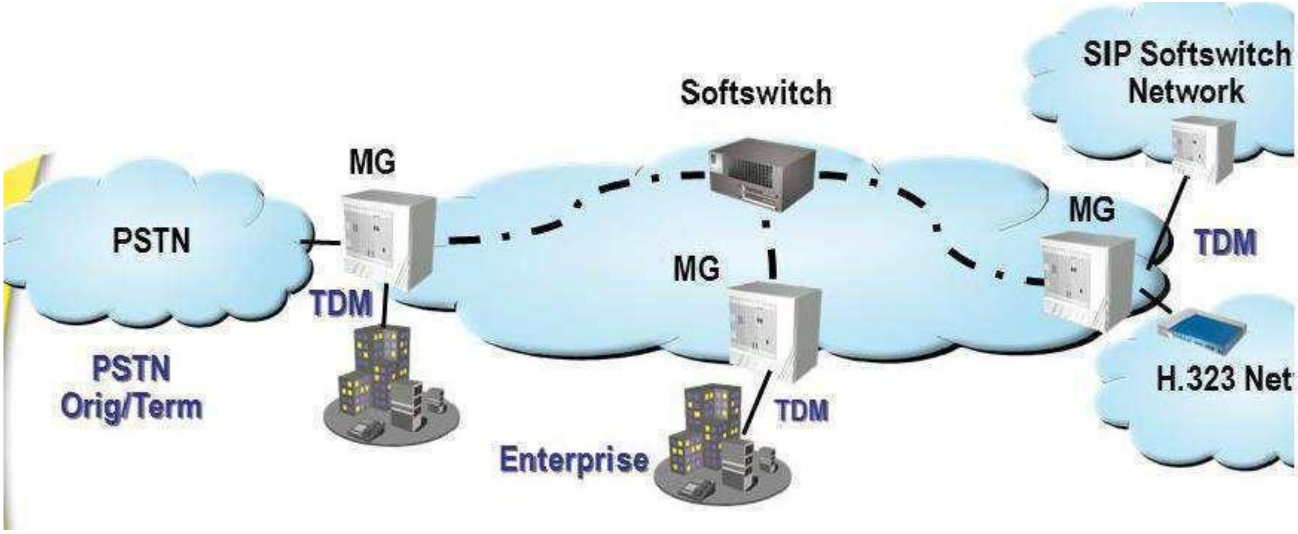


Fig 2.18

2.9 X.25

X.25 is a standard for WAN communications that defines how connections between user devices and network devices are established and maintained. X.25 is designed to operate effectively regardless of the type of systems connected to the network. It is typically used in the packet-switched networks (PSNs) of common carriers, such as the telephone companies. Subscribers are charged based on their use of the network.

X.25 network devices fall into three general categories: data terminal equipment (DTE), data circuit-terminating equipment (DCE), and packet-switching exchange (PSE).

Data terminal equipment (DTE) devices are end systems that communicate across the X.25 network. They are usually terminals, personal computers, or network hosts, and are located on the premises of individual subscribers. Data communication Equipments (DCEs) are communications devices, such as modems and packet switches that provide the interface between DTE devices and a PSE, and are generally located in the carrier's facilities.

Session Establishment

X.25 sessions are established when one DTE device contacts another to request a communication session. It’s up to the receiving DTE whether to accept or refuse the connection. If the request is accepted, the two systems begin full-duplex communication. Either DTE device can terminate the connection. After the session is terminated, any further communication requires the establishment of a new session.

Virtual Circuits

The X.25 is a packet-switched virtual circuit network. A virtual circuit is a logical connection created to ensure reliable communication between two network devices. A virtual circuit denotes the existence of a logical, bidirectional path from one DTE device to another across an X.25 network. Physically, the connection can pass through any number of intermediate nodes, such as DCE devices and PSEs. Virtual circuits in X.25 are created at the network layer such that multiple virtual circuits (logical connections) can be multiplexed onto a single physical circuit (a physical connection). Virtual circuits are demultiplexed at the remote end, and data is sent to the appropriate destinations.

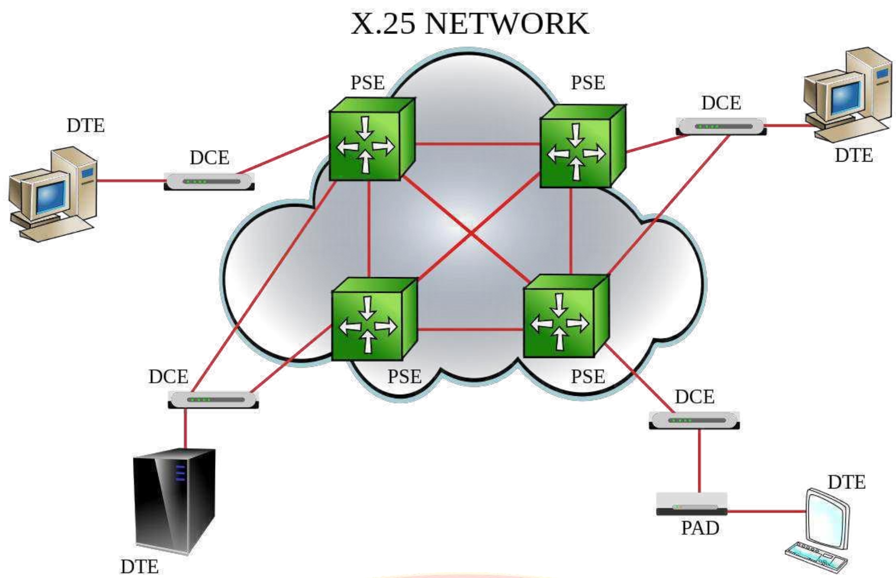


Fig 2.19

X.25 Protocol Suite

The X.25 protocol suite maps to the lowest three layers of the OSI reference model.
The layers are:

• Physical layer: Deals with the physical interface between an attached station and the link that attaches that station to the packet-switching node.
X.21 is the most commonly used physical layer standard.

• Frame layer: Facilitates reliable transfer of data across the physical link by transmitting the data as a sequence of frames. Uses a subset of HDLC known as Link Access Protocol Balanced (LAPB), bit oriented protocol.

• Packet layer: Responsible for end-to-end connection between two DTEs. Functions performed are:

1. Establishing connection
2. Transferring data
3. Terminating a connection
4. Error and flow control
5. With the help of X.25 packet layer, data are transmitted in packets over external virtual circuits.

2.9 INTEGRATED SERVICES DIGITAL NETWORK

Integrated Services Digital Network (ISDN) is a set of communication standards for simultaneous digital transmission of voice, video, data, and other network services over the traditional circuits of the public switched telephone network. Prior to ISDN, the telephone system was viewed as a way to transport voice, with some special services available for data. The key feature of ISDN is that it integrates speech and data on the same lines, adding features that were not available in the classic telephone system. The ISDN standards define several kinds of access interfaces, such as Basic Rate Interface (BRI), Primary Rate Interface (PRI), Narrowband ISDN (N-ISDN), and Broadband ISDN (B-ISDN).

ISDN is a circuit-switched telephone network system, which also provides access to packet switched networks, designed to allow digital transmission of voice and data over ordinary telephone copper wires, resulting in potentially better voice quality than an analog phone can provide. It offers circuit-switched connections (for either voice or data), and packet-switched connections (for data), in increments of 64 kilobit/s. In some countries, ISDN found major market application for Internet access, in which ISDN typically provides a maximum of 128 kbit/s bandwidth in both upstream and downstream directions. Channel bonding can achieve a greater data rate; typically the ISDN B-channels of three or four BRIs (six to eight 64 kbit/s channels) are bonded.

ISDN is employed as the network, data-link and physical layers in the context of the OSI model, or could be considered a suite of digital services existing on layers 1, 2, and 3 of the OSI model. In common use, ISDN is often limited to usage to Q.931 and related protocols, which are a set of signaling protocols establishing and breaking circuit-switched connections, and for advanced calling features for the user.

In a videoconference, ISDN provides simultaneous voice, video, and text transmission between individual desktop videoconferencing systems and group (room) videoconferencing systems.

The entry level interface to ISDN is the Basic Rate Interface (BRI), a 128 kbit/s service delivered over a pair of standard telephone copper wires.[4] The 144 kbit/s payload rate is broken down into two 64 kbit/s bearer channels ('B' channels) and one 16 kbit/s signaling channel ('D' channel or data channel). This is sometimes referred to as 2B+D.[5]

The interface specifies the following network interfaces:

The U interface is a two-wire interface between the exchange and a network terminating unit, which is usually the demarcation point in non-North American networks.

The T interface is a serial interface between a computing device and a terminal adapter, which is the digital equivalent of a modem.

The S interface is a four-wire bus that ISDN consumer devices plug into; the S & T reference points are

commonly implemented as a single interface labeled 'S/T' on a Network termination 1 (NT1).

The R interface defines the point between a non-ISDN device and a terminal adapter (TA) which provides translation to and from such a device.

BRI-ISDN is very popular in Europe but is much less common in North America. It is also common in Japan — where it is known as INS64.

The other ISDN access available is the Primary Rate Interface (PRI), which is carried over an E1 (2048 kbit/s) in most parts of the world. An E1 is 30 'B' channels of 64 kbit/s, one 'D' channel of 64 kbit/s and a timing and alarm channel of 64 kbit/s. This is often referred to as 30B+2D.

In North America PRI service is delivered on one or more T1 carriers (often referred to as 23B+D) of 1544 kbit/s (24 channels). A PRI has 23 'B' channels and 1 'D' channel for signalling (Japan uses a circuit called a J1, which is similar to a T1). Inter-changeably but incorrectly, a PRI is referred to as T1 because it uses the T1 carrier format. A true T1 (commonly called "Analog T1" to avoid confusion) uses 24 channels of 64 kbit/s of in-band signaling. Each channel uses 56 kb for data and voice and 8 kb for signaling and messaging. PRI uses out of band signaling which provides the 23 B channels with clear 64 kb for voice and data and one 64 kb 'D' channel for signaling and messaging. In North America, Non-Facility Associated Signalling allows two or more PRIs to be controlled by a single D channel, and is sometimes called "23B+D + n*24B". D-channel backup allows for a second D channel in case the primary fails. NFAS is commonly used on a T3.

PRI-ISDN is popular throughout the world, especially for connecting private branch exchanges to the public network.

Even though many network professionals use the term "ISDN" to refer to the lower-bandwidth BRI circuit, in North America BRI is relatively uncommon whilst PRI circuits serving PBXs are commonplac

Fig 2.20

UNIT-III

3.1 PHYSICAL LAYER –INTRODUCTION

The physical layer is the first layer of the Open System Interconnection Model (OSI Model). The physical layer deals with bit-level transmission between different devices and supports electrical or mechanical interfaces connecting to the physical medium for synchronized communication.

In the early 1960s, data communications was thought to mean digital data exchange between a centrally located mainframe computer and a remote computer terminal, or even between two terminals without a computer involved. These devices were linked by telephone voice lines, and therefore required a modem at each end for signal translation. Although a simple concept, the design was fairly complex to cater for the many opportunities for data error that occur when transmitting data through an analog channel.

A standard was needed to ensure reliable data communications, and to enable the interconnection of equipment produced by different manufacturers. From these factors, and to foster the benefits of mass production, a standards committee, known today as the Electronic Industries Association (EIA), developed the RS232 standard as a common interface standard for data communications equipment (generic).

The standard evolved over the years and in 1969 the third revision (RS-232C) became the standard of choice of PC makers. More recently the EIA232F standard was introduced in 1997 and the current V.24 and V.28 specifications were issued in 1996 and 1993 respectively. For the purpose of this report, it will be referred as RS 232.

To describe the RS 232 interface and to look at how its functionality relates to the Physical and Data Link Layers of the Open Systems Inter-Connect (OSI) model, we have to understand its physical and electrical properties. It will also look into how the data link layer directs the physical layer, in respect of the sender, and how the data link layer interprets the data received from the physical layer at the receiving end.

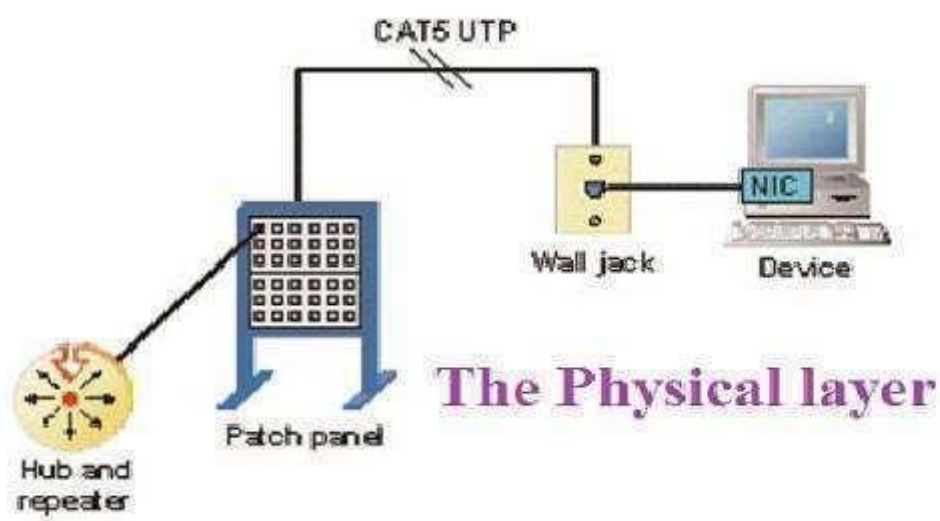


Fig.3.1

3.2INTERFACE

In communication studies, the notion of an interface in the work environment is used for a point of interaction between a number of systems or work groups. In the manufacturing environment, the coordination and interaction between several work groups is used to communicate plans and control production activity. This interaction can be schedules, human interactions, computer systems, or any other medium of communication. A physical interface is the interconnection between two items of hardware or machinery.

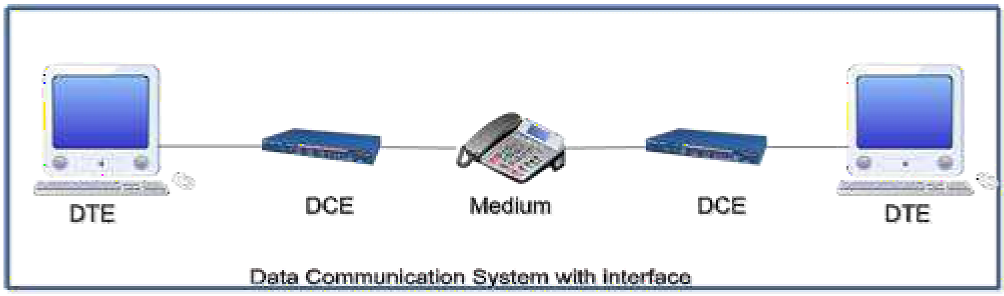


Fig.3.2

3.3 STANDARDS

There are two types of standards: formal and de facto. A formal standard is developed by an official industry or government body. For example, there are formal standards for applications such as Web browsers (e.g., HTTP, HTML), for network layer software (e.g., IP), data link layer software (e.g., Ethernet IEEE 802.3), and for physical hardware (e.g., V.90 modems). Formal standards typically take several years to develop, during which time technology changes, making them less useful.

De facto standards are those that emerge in the marketplace and are supported by several vendors but have no official standing. For example, Microsoft Windows is a product of one company and has not been formally recognized by any standards organization, yet it is a de facto standard. In the communications industry, de facto standards often become formal standards once they have been widely accepted.

International Telecommunications Union—Telecommunications Group The Telecommunications Group (ITU-T) is the technical standards-setting organization of the United Nations International Telecommunications Union, which is also based in Geneva (see **www.itu.int**). ITU is composed of representatives from about 200 member countries. Membership was originally focused on just the public telephone companies in each country, but a major reorganization in 1993 changed this, and ITU now seeks members among public- and private-sector organizations who operate computer or communications networks (e.g., RBOCs) or build software and equipment for them (e.g., AT&T).The RS 232 Standard.

American National Standards Institute The American National Standards Institute (ANSI) is the coordinating organization for the U.S. national system of standards for both technology and nontechnology (see www.ansi.org). ANSI has about 1,000 members from both public and private organizations in the United States. ANSI is a standardization organization, not a standards-making body, in that it accepts standards developed by other organizations and publishes them as American standards. Its role is to coordinate the development of voluntary national standards and to interact with ISO to develop national standards that comply with ISO's international recommendations. ANSI is a voting participant in the ISO.

3.4 EIA-232-D

The EIA 232D standard was developed in 1969 to specify the connections between a computer and a modem.
The term itself is an acronym which can be read as follows:
Electronics Industry Association (EIA) accepted standard, ID number 232 revision D
EIA 232D specifies the characteristics of the physical and electrical connections between two devices. Names and abbreviations are assigned to each pin or wire necessary for serial communications, for example:

Signal	Equip. Type	Symbol	Pin
Transmit Data	DCE	TxD	2
Receive Data	DTE	RxD	3
Request to Send	DCE	RTS	4

Signal	Equip. Type	Symbol	Pin
Clear to Send	DTE	CTS	5
Data Set Ready	DTE	DSR	6
Signal Ground		SG	7
Carrier Detect	DTE	CD	8
Data Terminal Ready	DCE	DTR	20
Ring Indicator	DTE	RI	22

Table 3.1

In EIA 232D, devices using pin 2 (TxD) for output (for example, computers and terminals) are given the name data terminal equipment (DTE). Devices using pin 2 (TxD) for input (for example, modems) are given the name data communication equipment (DCE).

EIA 232D also specifies the connectors. A DTE device normally has male connectors while DCE devices have female connectors. This standard is not always adhered to by manufacturers; therefore users should always review the device documentation before cable connection.

The RS 232 is the standard for the connection of the sending Data Terminal Equipment (DTE) and Data Communications Equipment (DCE) to the receiving DCE and DTE. A DTE is a device that forms part of the information processing of a system. Examples are a computer, terminal and printer. A DCE is a device that provides an interface between a DTE and a communications link, usually a modem. The RS 232 standards have developed to specify the interface between the DTE and DCE to include: Network and networking

Physical Layer

The physical layer defines the electrical, mechanical, procedural and functional specifications for activating, maintaining and deactivating the physical link between communicating network systems.

Within the physical layer, the RS 232 standard, defines the signalling levels, data rates, transmission distances and the physical connectors to be used. The primary reason for this is to enable the sending DTE/DCE to effectively communicate with the receiving DTE/DCE.

Signalling Levels

As stated earlier the physical layer converts the bit stream 0's and 1's into disturbances. Within the RS 232 standards the disturbances are represented as voltages along the transmission medium, usually copper wire between the sending and receiving DTE/DCE. The strength of the voltage travelling along the copper wire determines whether it recognised as a 0 or 1 by the receiving physical layer.This is graphically represented as follows:

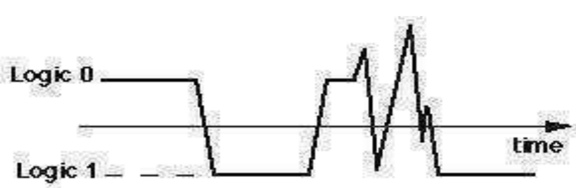


Fig. 3.3

The diagram shows that a 1 is represented by the electrical signal which is a negative voltage and a 0 is a positive voltage. The receiving physical layer is able to recognise these positive and negative voltages and convert them into a recognizable bit stream of which the data link layer can interpret. The passing of disturbances by the physical layer is graphically represented as

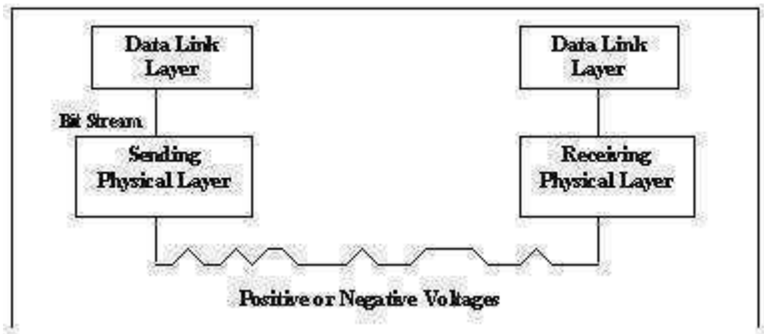


Fig. 3.4

As can be seen in this illustration, the sending physical layer converts the bit stream into voltages, transmits them along the transmission medium, the receiving physical layer recognises the voltages as either positive or negative and converts them back into 0's and 1's so they are recognisable by the data link layer.The specific voltage levels for the RS 232 standard are :

Table: Voltage Levels for the RS 232 Standatd

State	**Voltage Level TX**	**Voltage Level RX**
Logic 0	+5v to +15v	+3v to +25v
Logic 1	-5v to -15v	-3v to -25v

Fig. 3.5

The differences in the voltage become important when cable maximum lengths are being reached between DTE and DCE. The larger range of voltage at the receiver means it may be able to pick up a weaker signal which may have been caused by a long cable.

Physical Connectivity

This cables are used in past and was also country specific as , the Australian 240VAC standard male power connector has three rectangular prongs and is unique to Australia. Equipment which has the correct connector can be plugged in and should work anywhere in Australia. The unique connection system prevents overseas equipment with different connectors being plugged in as they are generally not compatible with the Australian power requirements. This prevents damage to the equipment.

For similar reasons as our power example, the RS 232 standard defines the requirements of the physical connectors which interconnect the DTE to the DCE and to the transmission medium. Having the correct connectors allows the equipment to be interconnected but does not necessarily make it work.Common connectors in use are as follows:

Fig. 3.6

The 25 pin RS 232 connector is the one defined in the standard.

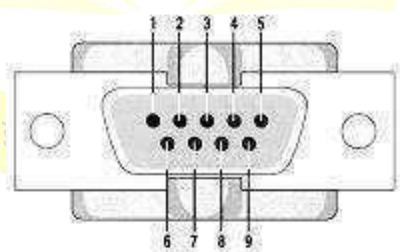


Fig. 3.7

This connector is nine pin RS 232 connector. On a PC, this is commonly referred to as the serial port.

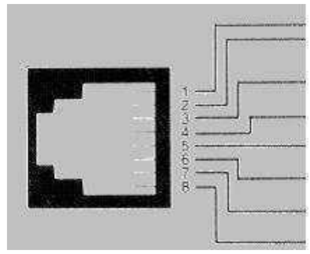


Fig. 3.8

This connector is a modular 9 pin connector, commonly known as an RJ 45 connection. The connectors allow the physical components to interconnect; however, how the cabling is wired to the various pins determines whether the sending and receiving physical layers will be able to communicate.

A 9 pin connector will be used to explain how the physical layers communicate.

Fig. 3.9

DTE

1. at the physical layer it can be a terminal, computer, printer, fax etc
2. sends data on Transmitted Data (TxD) line

3.4

1. receives on Received Data (RxD) line
2. asserts Request to Send (RTS) when ready to receive
3.
4. waits for Clear To Send (CTS) to be asserted before sending
5. asserts Data Terminal Ready (DTR) when ready and waiting (to receive)
6. expects Data Set Ready (DSR) to be asserted before performing (sending)
7. expects Data Carrier Detect (DCD) to be asserted before receiving

DCE

At the physical layer the DCE takes the bit stream converts them into a signal (voltages) and then introduces the signal onto the telecommunications medium. Normally the DCE is known as a modem.
the wiring is the inverse as that of the DTE.
The most important lines are RxD, TxD, and SG; the others are used with modems, printers and plotters to indicate internal states.

RTS and CTS Lines

The RTS and CTS are used by the physical layer to start or stop a transmission. The DTE/DCE starts the transmission by sending a voltage of -5 to -15 down (binary 1) the RTS line. Once the receiving physical layer receives the signal it responds by sending a negative voltage -5 to -15 (binary 1) down CTS line. If the physical layer wants to stop or interrupt the transmission it sends a +5v to 15v (binary 0) down the CTS line. In this way the physical layer is able to control the flow of data.

DTR and DSR Lines

DTR and DSR are used to establish a connection between the physical layers at the very beginning. A good way of looking at is as "handshaking" of the modems at the sending and receiving physical layers. The sending physical layer sets DTR to binary 1 by sending a negative -5v to 15 v down the line, and receiving physical layer answers with a binary 1 by sending a -5v to 15v down the DSR line. This indicates that flow of data (represented by voltages) between the physical layers can commence.

SG

The Signal to ground is the logical ground which is used as a reference point for all signals received or transmitted.
Note that the above seven lines are often referred to as the "7-wire connection", or "hand-shake connection."

DCD

The modem uses this line to indicate that it has detected the carrier of the modem on the other side of the phone line. Voltages, once again are used to do this.

Transmission Distances

Cable length standards are important to protect the integrity of the signal and to allow sending and receiving DTE/DCE to communicate effectively. A good example to understand why this is the case is to think of a person yelling down a piece of PVC pipe, the longer the pipe the weaker his voice will be at the receiving end. The same is true with data communications, the longer the cable the weaker the signal becomes at the receiving end. It is for this reason that the voltage range is greater at the receiving end than the transmitting end, it allows for the degradation of the signal (weaker voltages).
RS 232 standard sets the maximum cable length as 15 metres between a DTE and DCE for signaling rates < 20 kbps. This standard is designed to ensure maximum communication speed can occur, longer cable distances can be achieved but the data rate will be reduced as a consequence. However, since this standard was written cable quality has improved considerably which now allows much grater distances to be achieved.
Much larger distances are achieved once the signal is forwarded onto the transmission lines of a telecommunication system e.g. PSTN line, as the signal is regenerated through signal boosters and optical isolators.

3.5 RJ-45

Connector	Length	Width	Height

4P4C (RJ9)		7.7	
6P4C (RJ11)	12.34	9.65	6.60
8P8C (RJ45)	21.46	11.68	8.30

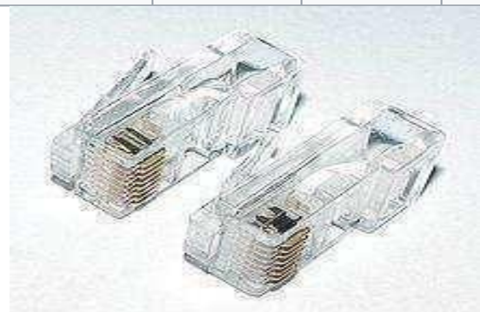


Fig 3.10

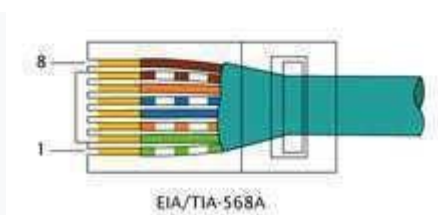
8P8C (8 position 8 contact)

The 8 position 8 contact (8P8C) connector is a modular connector commonly used to terminate twisted pair and multi-conductor flat cable. These connectors are commonly used for Ethernet over twisted pair, registered jacks and other telephone applications, RS-232 serial using the EIA/TIA-561 and Yost standards, and other applications involving unshielded twisted pair, shielded twisted pair, and multi-conductor flat cable.

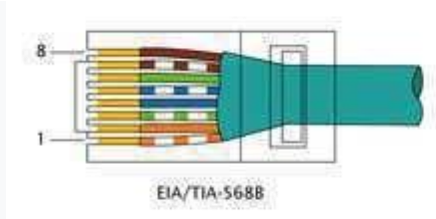
An 8P8C modular connection has two paired components: the male plug and the female jack, each with eight equally-spaced conductors. On the plug, these conductors are flat contacts positioned parallel with the connector body. Inside the jack, the contacts are suspended diagonally toward the insertion interface. When an 8P8C plug is mated with an 8P8C jack, the contacts meet and create an electrical connection. Spring tension in the jack's contacts ensures a good interface with the plug and allows for slight travel during insertion and removal.

Although commonly referred to as an RJ45 in the context of Ethernet and category 5 cables, it is incorrect to refer to a generic 8P8C connector as an RJ45. A telephone-system-standard RJ45 plug has a key which excludes insertion in an un-keyed 8P8C socket. The registered jack (RJ) standard specifies a different mechanical interface and wiring scheme for an RJ45S from TIA/EIA-568-B which is often used for modular connectors used in Ethernet and telephone applications. 8P8C modular plugs and jacks look very similar to the plugs and jacks used for FCC's registered jack RJ45 variants, although the RJ45S is not compatible with 8P8C modular connectors.

Pinout



T568A wiring



T568B wiring

Fig 3.11

Connectors are frequently terminated using the T568A or T568B assignments that are defined in TIA/EIA-568. The drawings to the right show that the copper connections and pairing are the same, the only difference is that the orange and green pairs (colors) are swapped. A cable wired as T568A at one end and T568B at the other (Tx and Rx pairs reversed) is a "crossover" cable. Before the widespread acceptance of auto MDI-X capabilities a crossover cable was needed to interconnect similar network equipment (such as Ethernet hubs to Ethernet hubs). A cable wired the same at both ends is called a "patch" or "straight-through" cable, because no pin/pair assignments are swapped. Crossover cables are sometimes still used to connect two computers together without a switch or hub, however most network interface cards (NIC) in use today implement auto MDI-X to automatically configure themselves based on the type of cable plugged into them. If a "patch" or "straight" cable is used to connect two computers with auto MDI-X capable NICs, one NIC will configure itself to swap the functions of its Tx and Rx wire pairs.

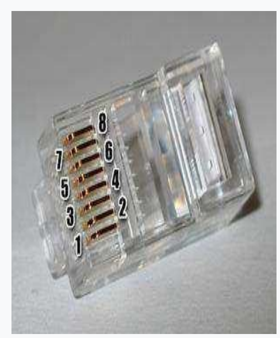
Pin	T568A pair	T568B pair	10/100BASE-T signal id.	1G/10GBASE-T signal id.	Wire	T568A color	T568B color	Diagram
1	3	2	DA+	DA+	tip	white/green stripe	white/orange stripe	
2	3	2	DA−	DA−	ring	green solid	orange solid	
3	2	3	DB+	DB+	tip	white/orange stripe	white/green stripe	
4	1	1	NC	DC+	ring	blue solid	blue solid	
5	1	1	NC	DC−	tip	white/blue stripe	white/blue stripe	
6	2	3	DB−	DB−	ring	orange solid	green solid	Pin numbering on plug. Connected pins on plug and jack have the same number.
7	4	4	NC	DD+	tip	white/brown stripe	white/brown stripe	
8	4	4	NC	DD−	ring	brown solid	brown solid	

Fig 3.12

3.6 RJ-11

RJ-11. (Registered Jack-11) A telephone interface that uses a cable of twisted wire pairs and a modular jack with two, four or six contacts. RJ-11 is the common connector for plugging a telephone into the wall and the handset into the telephone. A telephone interface that uses a cable of twisted wire pairs and a modular jack with two, four or six contacts. RJ-11 is the common connector for plugging a telephone into the wall and the handset into the telephone.

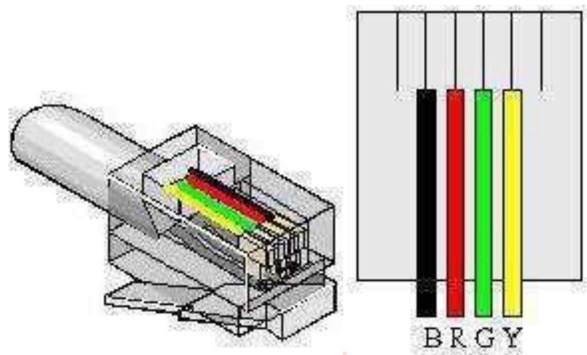


Fig 3.13

The diagram is shown with the "hook clip" on the underside. The typical RJ-11 connector has six terminals. Usually, only the middle four pins are used. The POTS (Plain Old Telephone Service) residential telephone wiring generally contains two pairs of wires - designed for two separate telephone lines. The center pins (Red and Green) contain the first telephone line. Please note that business (digital) phone systems may be wired differently.

3.7 BNC CONNECTOR

The BNC (Bayonet Neill–Concelman) connector is a miniature quick connect/disconnect radio frequency connector used for coaxial cable. It features two bayonet lugs on the female connector; mating is fully achieved with a quarter turn of the coupling nut. BNC connectors are used with miniature-to-subminiature coaxial cable in radio, television, and other radio-frequency electronic equipment, test instruments, and video signals. The BNC was commonly used for early computer networks, including ARCnet, the IBM PC Network, and the 10BASE2 variant of Ethernet. BNC connectors are made to match the characteristic impedance of cable at either 50 ohms or 75 ohms. They are usually applied for frequencies below 4 GHz[1] and voltages below 500 volts.

The BNC uses a slotted outer conductor and some plastic dielectric on each gender connector. This dielectric causes increasing losses at higher frequencies. Above 4 GHz, the slots may radiate signals, so the connector is usable, but not necessarily stable up to about 11 GHz. Both 50 ohm and 75 ohm versions are available. The BNC connector is used for signal connections such as:

A. analog and serial digital interface video signals
B. amateur radio antennas
C. aerospace electronics (avionics)
D. test equipment.

BNC Tee Connectors with resistive load terminators

The BNC connector is used for composite video on commercial video devices. Consumer electronics devices with RCA connector jacks can be used with BNC-only commercial video equipment by inserting an adapter. BNC connectors were commonly used on 10base2 thin Ethernet network cables and network cards. BNC connections can also be found in recording studios. Digital recording equipment uses the connection for synchronization of various components via the transmission of word clock timing signals.

Typically the male connector is fitted to a cable, and the female to a panel on equipment. Cable connectors are often designed to be fitted by crimping[4] using a special power or manual tool. Wire strippers which strip outer jacket, shield braid, and inner dielectric to the correct lengths in one operation are used.

Fig 3.14

Types

BNC connectors are most commonly made in 50 and 75 ohm versions, matched for use with cables of the same characteristic impedance. The 75 ohm types can sometimes be recognized by the reduced or absent dielectric in the mating ends but this is by no means reliable. There was a proposal in the early 1970s for the dielectric material to be coloured red in 75 ohm connectors, and while this is occasionally implemented, it did not become standard. The 75 ohm connector is dimensionally slightly different from the 50 ohm variant, but the two nevertheless can be made to mate. The 50 ohm connectors are typically specified for use at frequencies up to 4 GHz and the 75 ohm version up to 2 GHz. A 95 ohm variant is used within the aerospace sector, but rarely elsewhere. It is used with the 95 ohm video connections for glass cockpit displays on some aircraft.

Video (particularly HD video signals) and DS3 Telco central office applications primarily use 75 ohm BNC connectors, whereas 50 ohm connectors are used for data and RF. Many VHF receivers used 75 ohm antenna inputs, so they often used 75 ohm BNC connectors.

Reverse-polarity BNC (RP-BNC) is a variation of the BNC specification which reverses the polarity of the interface. In a connector of this type, the female contact normally found in a jack is usually in the plug, while the male contact normally found in a plug is in the jack. This ensures that reverse polarity interface connectors do not mate with standard interface connectors. The SHV connector is a high-voltage BNC variant that uses this reverse polarity configuration.

Smaller versions of the BNC connector, called Mini BNC and High Density BNC (HD BNC), are manufactured by Amphenol. While retaining the electrical characteristics of the original specification, they have smaller footprints giving a higher packing density on circuit boards and equipment backplanes. These connectors have true 75 ohm impedance making them suitable for HD video applications.

EIA-449 Digital Interface

The RS-449 specification, also known as EIA-449 or TIA-449, defines the functional and mechanical characteristics of the interface between data terminal equipment and data communications equipment. The electrical signaling standards intended for use with RS-449 are RS-422 for balanced signals, and RS-423 for the unbalanced signals, with data rates to 2 Mbit/s. The standard specifies DC-37 and DE-9 for the primary and secondary data circuits. Though never applied on personal computers, this interface is found on some network communication equipment. The full title of the standard is EIA-449 General Purpose 37-Position and 9-Position Interface for Data Terminal Equipment and Data Circuit-Terminating Equipment Employing Serial Binary Data Interchange.

Interface Standards

RS-449 (often written as RS449) is a specification for a differential communications interface that uses a DB-37 connector and differential equivalents of the V.24 (RS-232) signals. Some of the link management control signals are implemented using V.10 (RS-423) single ended interfaces. Note that the EIA standards have effectively replaced the RS standards. Note also that RS-449 and EIA-449 (often written as EIA449) are also sometimes referred to as V.36 (a modem standard that specifies an RS-449 type data interface).

Interface Characteristics

RS-449 is a differential communications interface used for synchronous communications with some single-ended link management signals, typically limited to a maximum throughput of 10Mbps. Communications over distances exceeding 1000m is possible at low bit rates, the actual performance being mostly dependent on cable specification. Separate clock lines are used for receiving and transmitting data.

Interface Applications

RS-449 interfaces are commonly found on communications equipment in some parts of the world where high throughput and/or long distances are required. The interface also offers good noise immunity enabling reliable communications in environments where there are high levels of EMI (electromagnetic interference).

Interface Connector Types and Pinouts

The signals used by the overwhelming majority of applications are marked in bold.

Signal Name	DB37 Contact	Supported on FarSync cards
Shield	1	Yes
Signal Rate Indicator	2	
Unassigned	3	
Send Data (A)	4	Yes
Send Timing (A)	5	Yes
Receive Data (A)	6	Yes
Request To Send (A)	7	Yes
Receive Timing (A)	8	Yes
Clear To Send (A)	9	Yes
Local Loopback	10	
Data Mode (A)	11	
Terminal Ready (A)	12	
Receiver Ready (A)	13	
Remote Loopback	14	
Incoming Call	15	
Select Frequency	16	
Terminal Timing (A)	17	
Test Mode	18	
Signal Ground	19	Yes
Receive Common	20	

Unassigned	21		
Send Data (B)	22	Yes	
Send Timing (B)	23		Yes
Receive Data (B)	24		Yes
Request To Send (B)	25		Yes
Receive Timing (B)	26		Yes
Clear To Send (B)	27		Yes
Terminal In Service	28		
Data Mode (B)	29		
Terminal Ready (B)	30		
Receiver Ready (B)	31		
Select Standby	32		
Signal Quality	33		
New Signal	34		
Terminal Timing (B)	35		
Standby Indicator	36		
Send Common	37		

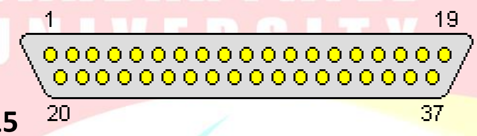


Fig 3.15

3.8 X.21 MODEMS

X.21 (sometimes referred to as X21) is an interface specification for differential communications introduced in the mid-1970s by the ITU-T. X.21 was first introduced as a means to provide a digital signaling interface for telecommunications between carriers and customers' equipment. This includes specifications for DTE/DCE physical interface elements, alignment of call control characters and error checking, elements of the call control phase for circuit switching services, and test loops.

When X.21 is used with V.11, it provides synchronous data transmission at rates from 600 bit/s to 10 Mbit/s. There is also a variant of X.21 that is only used in select legacy applications, “circuit switched X.21”. X.21 normally is found on a 15-pin D-Sub connector and is capable of running full-duplex data transmissions.

The Signal Element Timing, or clock, is provided by the carrier (telephone company), and is responsible for correct clocking of the data. X.21 is primarily used in Europe and Japan, for example in the Scandinavian DATEX and German DATEX-L circuit switched networks during the 1980s.

Fig 3.16

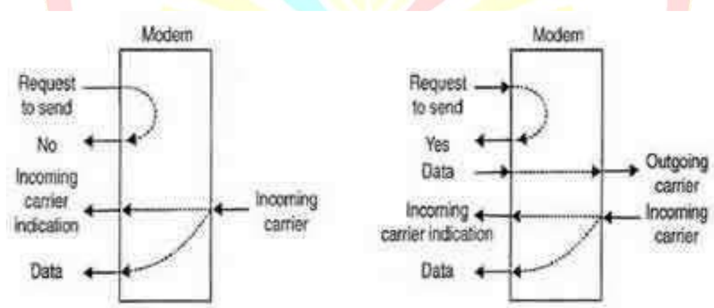
Cables using this pinout are known as X.21 Null-Modem or Crossover cables, they can be used as a low cost way to replace a pair of synchronous X.21 modems or a synchronous X.21 modem eliminator as long as the device at one end of the cable can product the clocks. Both the FarSync T2P and T4P cards can be configured to generate the required clock signals (Sa/Sb) on pins 6 and 13.

```
15 Pin D type female                  15 Pin D type female

Shield    1 ----------------------  1  Shield
Ta        2 ----------------------  4  Ra
Ca        3 ----------------------  5  Ia
Ra        4 ----------------------  2  Ta
Ia        5 ----------------------  3  Ca
Sa        6 ----------------------  6  Sa
Sig Gnd   8 ----------------------  8  Sig Gnd
Tb        9 ---------------------- 11  Rb
Cb       10 ---------------------- 12  Ib
Rb       11 ----------------------  9  Tb
Ib       12 ---------------------- 10  Cb
Sb       13 ---------------------- 13  Sb


            <----- 0.5 metres ---->
```


3.8 aTypes of X.25 Modem and its features
Interface Standards

There are many different types of modems. They are also classified through numerous ways. However, generally the classification is based on the basic function of a modem. Some of the common types are –

On the basis of directional capability, modems are divided into half duplex and full duplex typesHalf duplex modem is each station can transmit and receive but not at the same time, while full duplex modem is both stations can transmit and receive simultaneously.



(a) Half Duplex Modem (b) Full Duplex Modem

Fig 3.17

On the basis of connection to the line they are classified into 2 wire and 4 wire modem types.

2 wire modem – These modems make use of the same pair of wires for outgoing and incoming carriers. Due to the use of only one pair of wires which is extended into the subscriber's location, this type of leased 2 wire connection is less expensive than the 4 wire connection.

- 2-wire modems use the same pair of wires for outgoing and incoming carriers.
- A leased 2-wireconrlection is usually cheaper than a 4-wire connection as only one pair of wires is extended to the subscriber's premises.
- The data connection established through telephone exchange is also a 2-wire connection.

• In 2-wire modems, half duplex mode of transmission that uses the same frequency for the incoming and outgoing carriers can be easily implemented.
• For full duplex mode of operation, it is necessary to have two transmission channels, one for transmit direction and the other for receive direction.
• This is achieved by frequency division multiplexing of two different carrier frequencies. These carriers are placed within the bandwidth of the speech channel.

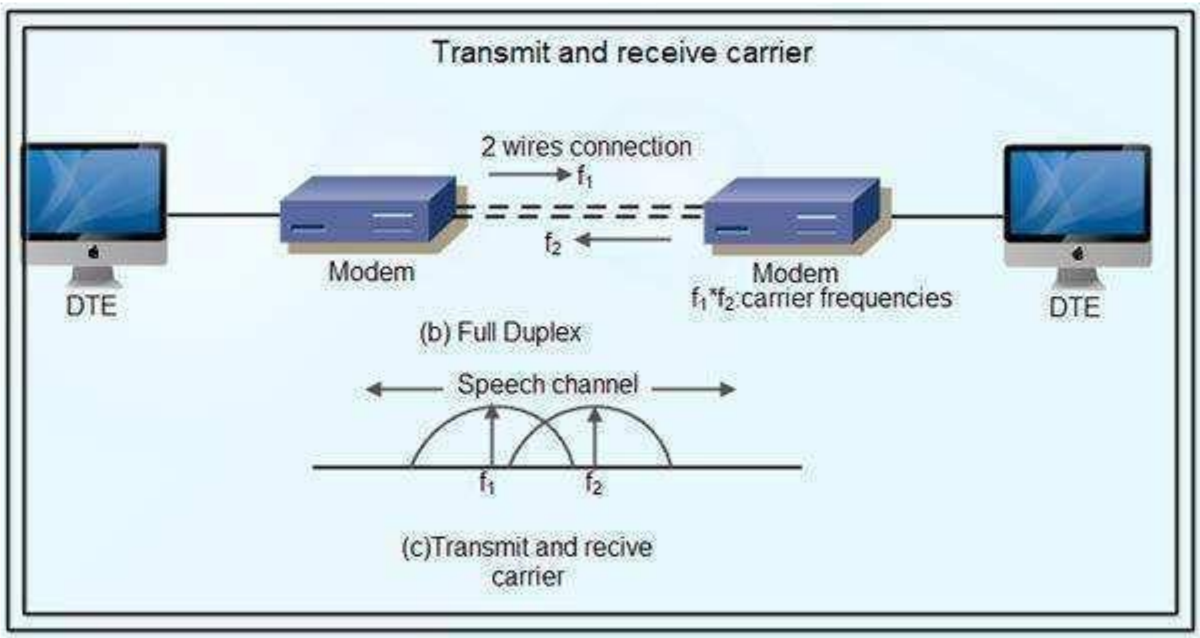
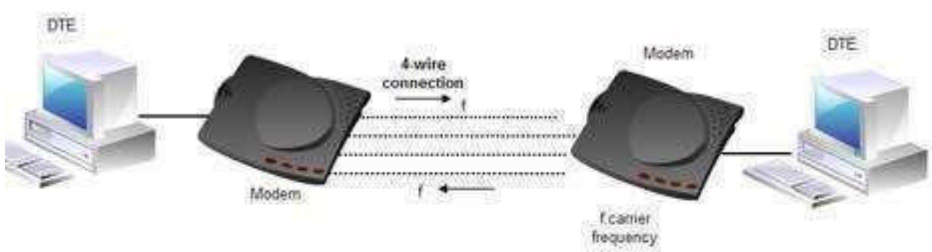


Fig 3.18



4wire-Modem

Fig 3.19

4 wire modem – In this type of connection, separate wires are used for incoming and outgaining carrier. Data can be transmitted on half and full duplex mode through these settings. The same carrier frequency can be used for transmission in both directions as the physical path is separate for each in this case.

On the basis of transmission mode, modems are divided into asynchronous and synchronous types-

Synchronous Modem - Data is transmitted in frames along with synchronization bits which are used for ensuring the timely transmission and reception of data. These modems are mainlyemployed on dedicated leased lines.

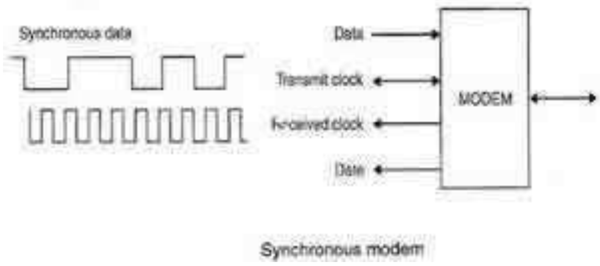


Fig 3.20

Asynchronous Modem – In these types of modems, every byte is positioned between a stop and a start bit. This lacks the timing signal or clock between modem and DTE. It is able to manage a continuous flow of data bits provided that a clock signal is used.

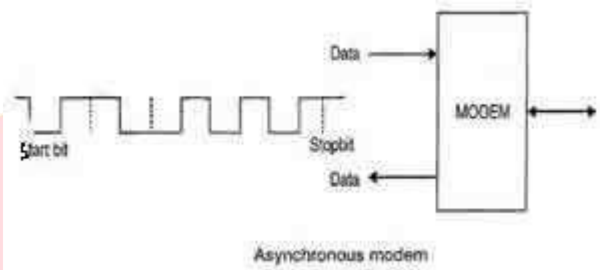


Fig 3.21

3.9 BLOCK SCHEMATIC OF MODEM

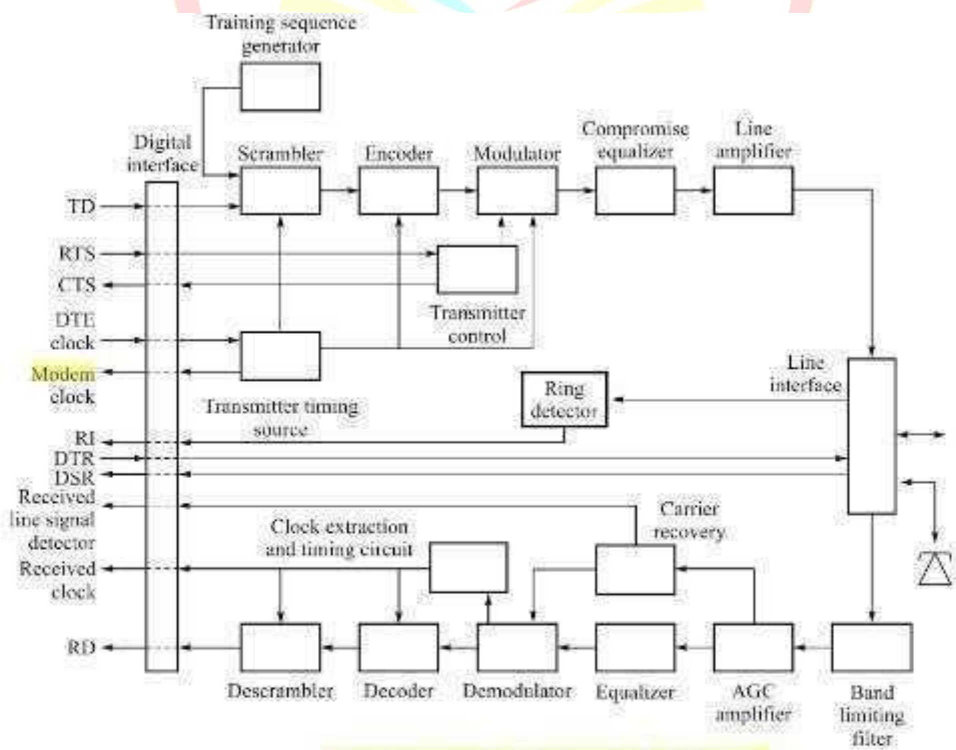


Fig 3.22

X.21 (occasionally written as X21)is a specification for differential communications that that includes the definition of connector pin allocations. It is used together with V.11 to define a specification for serial synchronous communications at up to 10Mbps. A variant of X.21 called 'circuit switched X.21' is now no longer in use except for a few legacy systems.

V.11 is a specification for differential communications that defines signal electrical characteristics. Signals meeting V.11 requirements are used in X.21, RS-449 (EIA-449), RS-530 (EIA-530) and the balanced signal part of V.35 interfaces.

RS-422(often written as RS422)is essentially equivalent to V.11. Note that the EIA standards have effectively replaced the RS standards.

3.10SIGNAL CONSTELLATION

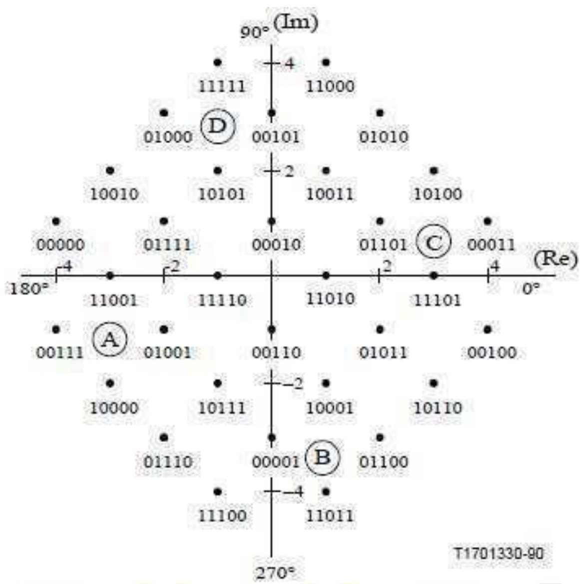


Fig 3.23

At 4800 bits per second, the scrambled data stream to be transmitted is divided into groups of two consecutive data bits. The two bits Q1n and Q2n, where Q1n is first in time, where the subscript n designates the sequence number of the group, are first differentially encoded into Y1n and Y2n according to Table 2/V.32 bis. The two differentially encoded bits Y1n and Y2n are then mapped into the coordinates of the signal element to be transmitted according to the signal space diagram shown in Figure_/V.32 bis.

Interface Characteristics

X.21 is a differential interface, typically limited to a maximum throughput of 10Mbps. Communications over distances exceeding 1000m is possible at low bit rates, the actual performance being mostly dependent on cable specification. A single clock signal is used for receiving and transmitting data.

Interface Applications

X. 1/V.11 interfaces are used where high throughput and/or long distances are required. Commonly used bit-rates for synchronous communications are 64Kbps, 128Kbps, 256Kbps etc. The interface also offers good noise immunity enabling reliable communications in environments where there are high levels of EMI (electromagnetic interference). Typical protocols used over X.21 interfaces are HDLC, X.25, SNA and PPP.

In some common applications including industrial controls, RS-422 interfaces are used to extend the reach of asynchronous communications, with differential drivers and receivers used instead of RS-232 devices for the line interfaces. Asynchronous RS-422 applications normally use a DB9 connector although the pin assignments are not standardised.

Signal Ground (G) -	This provides reference for the logic states against the other circuits. This signal may be connected to the protective ground (earth).
DTE Common Return (Ga) -	Used only in unbalanced-type configurations (X.26), this signal provides reference ground for receivers in the DCE interface.
Transmit (T) -	This carries the binary signals which carry data from the DTE to the DCE. This circuit can be used in data-transfer phases or in call-control phases from the DTE to DCE (during Call Connect or Call Disconnect).
Receive (R) -	Controlled by the DTE to indicate to the DCE the meaning of the data sent on the transmit circuit. This circuit must be ON during data-transfer phase and can be ON or OFF during call-control phases, as defined by the protocol.
Indication (I) -	The DCE controls this circuit to indicate to the DTE the type of data sent on the Receive line. During data phase, this circuit must be ON and it can be ON or OFF during call control, as defined by the protocol.
Signal Element Timing (S) -	This provides the DTE or DCE with timing information for sampling the Receive line or Transmit line. The DTE samples at the correct instant to determine if a binary 1 or 0 is being sent by the DCE. The DCE samples to accurately recover signals at the correct instant. This signal is always ON.
Byte Timing (B) -	This circuit is normally ON and provides the DTE with 8-bit byte element timing. The circuit transitions to OFF when the Signal Element Timing circuit samples the last bit of an 8-bit byte. Call-control characters must align with the B lead during call-control phases. During data- transfer phase, the communicating devices bilaterally agree to use the B lead to define the end of each transmitted or received byte. The C and I leads then only monitor and record changes in this condition when the B lead changes from OFF to ON, although the C and I leads may be altered by the transitions on the S lead. This lead is frequently not used.

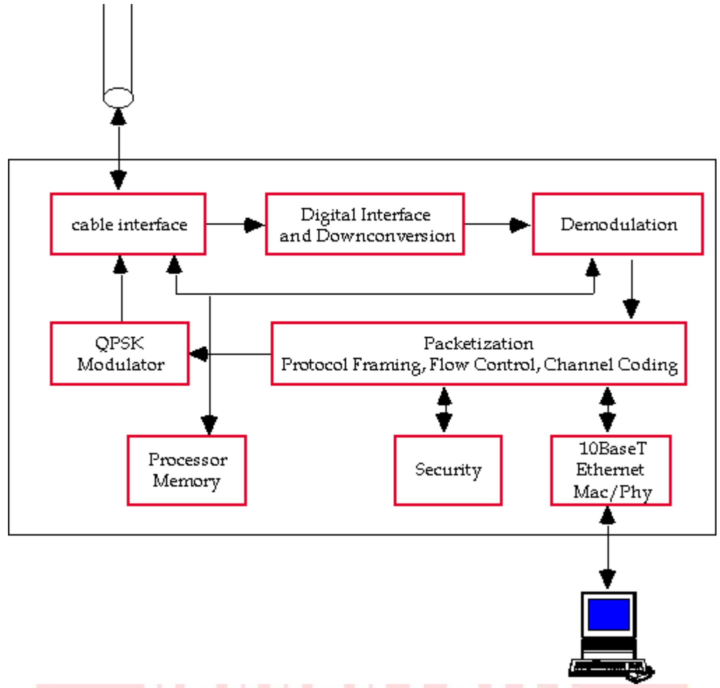


Fig 3.24

List of ITU-T V-series recommendations

a) The ITU-T V-Series Recommendations on Data communication over the telephone network specify the protocols that govern approved modem communication standards and interfaces.
b) V.1 is an ITU-T recommendation, entitled Equivalence between binary notation symbols and the significant conditions of a two-condition code.
c) V.2 is an ITU-T recommendation, approved in November 1988, titled Power levels for data transmission over telephone lines.
d) V.4 is an ITU-T recommendation, approved in November 1988, titled General structure of signals of International Alphabet No. 5 code for character oriented data transmission over public telephone networks.
e) V.5 was an ITU-T recommendation, approved in November 1988, titled Standardization of data signalling rates for synchronous data transmission in the general switched telephone network. It has been withdrawn since.
f) V.6 was an ITU-T recommendation, approved in November 1988, titled Standardization of data signalling rates for synchronous data transmission on leased telephone-type circuits. It has been withdrawn since.
g) V.7 is an ITU-T recommendation, approved in November 1988, titled Definitions of terms concerning data communication over the telephone network.
h) V.8 is an ITU-T recommendation, first approved in September 1994, titled Procedures for starting sessions of data transmission over the public switched telephone network. It has been superseded three times. The current version was approved in November 2000.
i) V.8bis is an ITU-T recommendation, first approved in August 1996, titled Procedures for the identification and selection of common modes of operation between data circuit-terminating equipments (DCEs) and between data terminal equipments (DTEs) over the public switched telephone network and on leased point-to-point telephone-type circuits. It has been superseded twice. The current version was approved in November 2000.

Active and Passive Hub

A central connecting device in a network that regenerates signals on the output side to keep the signal strong.Also called a "multiport repeater." Contrast with passive hub and intelligent hub.

These hubs are nothing more than point contacts for the wires that make up the physical network. An example of this is a punch-down block that is a simple plastic, unpowered box used to plug network cables into.Passive Hub works like a simple Bridge. It is used for just creating a connection regenerate any incoming signal. It receives signal and then forward it to multiple devices between various devices. It does not have It

has the ability to amplify or

Fig 3.25

Active hubs are a little smarter than passive hubs. You might also come across the term "concentrators," which are basically active hubs that concentrate and strengthen a signal as it enters and exits the hub.Active Hub is a hub which can amplify or regenerate the information signal. This type of bus has an advantage as it

also amplifies the incoming signal as well as forward it to multiple devices. This Bus is also known as Multiport Repeater. It can upgrade the properties if incoming signal before sending them to destination.

Asynchronous Modem

- Asynchronous modems can handle data bytes with start and stop bits.
- There is no separate timing signal or clock between the modem and the DTE.
- The internal timing pulses are synchronized repeatedly to the leading edge of the start pulse .

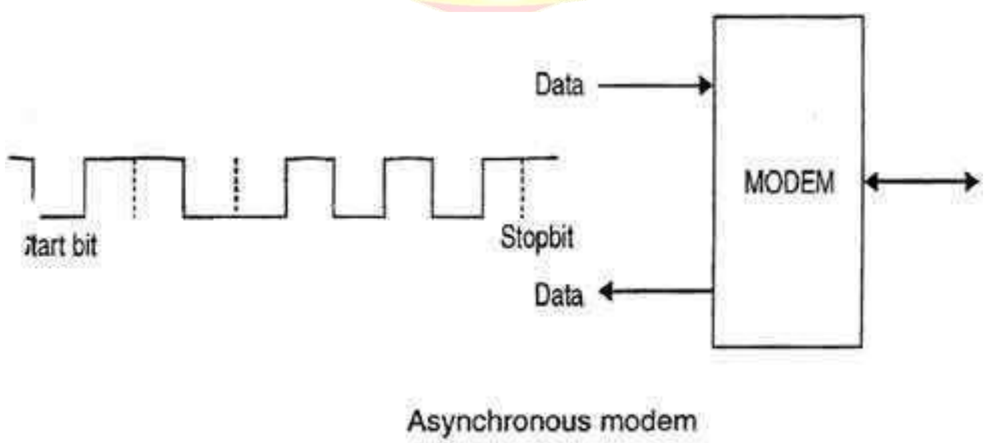


Fig. 3.26

Synchronous Modem

• Synchronous modems can handle a continuous stream of data bits but requires a clock signal.
• The data bits are always synchronized to the clock signal.
• There are separate clocks for the data bits being transmitted and received.
• For synchronous transmission of data bits, the DTE can use its internal clock and supply the same to the modem.

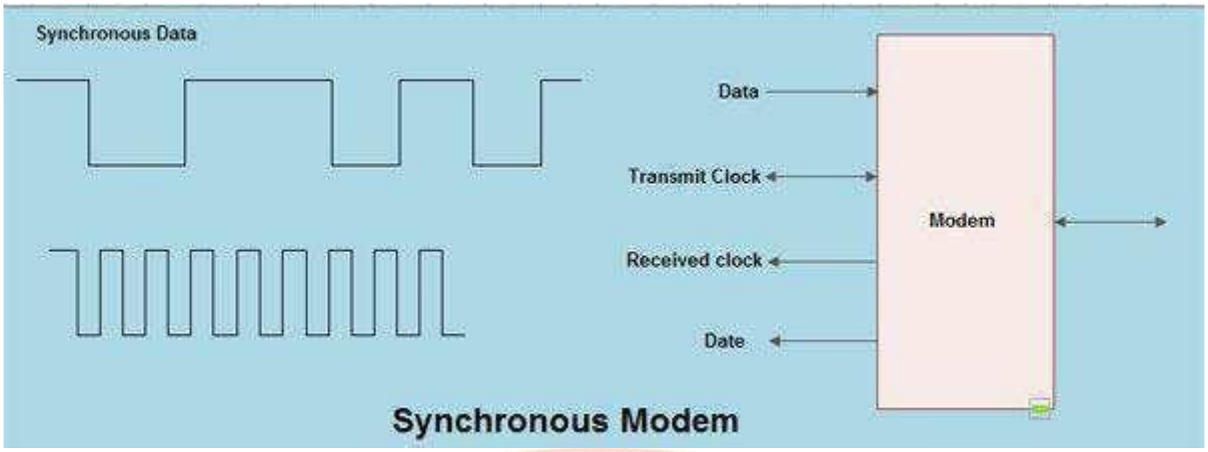


Fig. 3.27

Modulation techniques used for Modem:

The basic modulation techniques used by a modem to convert digital data to analog signals are :
• Amplitude shift keying (ASK).
• Frequency shift keying (FSK).
• Phase shift keying (PSK).
• Differential PSK (DPSK).
These techniques are known as the binary continuous wave (CW) modulation.
• Modems are always used in pairs. Any system whether simplex, half duplex or full duplex requires a modem at the transmitting as well as the receiving end.
• Thus a modem acts as the electronic bridge between two worlds - the world of purely digital signals and the established analog world.

A dial-up is a connection that is established using a modem. To make the dial-up connection the modem must be connected to an active phone line that is not in use. When connecting the modem will pick up the phone and dial a number that is attached to another computer. After the connection has been made the computer can check e-mail, browse the Internet, and share files.

Fig. 3.28

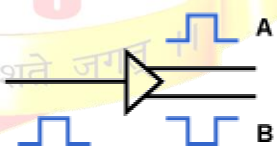
Today, with multimedia and bigger web pages on the Internet most users have an un-enjoyable time browsing the Internet using a dial-up connection and try to use other options. Most users who have the available option use some form of broadband connection, which allows a much faster download and upload.

Baseband Modem is a digital modem that may be used to inter-connect computers, terminals, controllers and similar digital equipment over distances of up to 16 kms (10 miles) for LAN interconnection, campus networking, or high speed leased line internet links, over a single, un-conditioned twisted copper pair (two wires). These devices overcome distance limitation and noise problems by using special modulation and line equalization techniques and allow error-free communication over longer distances, at much higher data rates than conventional analog dial-up modems. VCL - Baseband Modems provide a cost effective and efficient solutions for dedicated data-network access and for the "last mile" network access applications.

	Highlights	**Features**
1.	Campus LAN & WAN connections	Covers distances of 16 kms on a single, unconditioned twisted (10 miles) pair (two wires)
2.	Offers data rates of 115.2Kbps,	High speed leased line internet links Asynchronous
3.	Offers data rates of 64 and128 Kbps,	LAN interconnection Synchronous
4.	Choice of interfaces	Campus networking
5.	Supports point-to-point synchronous or asynchronous communication	Local analog and remote digital loopback tests

A line driver is an electronic amplifier circuit designed for driving a load such as a transmission line. The amplifier's output impedance may be matched to the characteristic impedance of the transmission line. Line drivers are commonly used within digital systems, e.g. to communicate digital signals across circuit-board traces and cables. In analog audio, a line driver is typically used to drive line-level analog signal outputs, for example to connect a stereo music player to an amplified speaker system.

Line drivers offer the simplest and cheapest method of increasing the distance between two devices. The simplest line drivers convert digital pulses from a single signal into a differential signal. This signal offers a number of advantages. Line drivers are suitable for use over 2- or 4-wire direct cabling (privately owned lines).



Line Drivers:

SPEED	★★★	1 - 100 k
DISTANCE	★★	0 - 4 km
QUICK INSTALL	★★★★★	5 - 10 mn

Fig. 3.29

Distance can be as far as 4 km since the receive circuitry can detect minute differences between the A and B wires. Interference effects A and B wires equally, meaning the difference stays the same and the data is uncorrupted.

Modems -use an analogue wave signal to carry data over the phone lines (modulation/demodulation). The speed is limited by the bandwidth offered by the public switched telephone network (PSTN), which was originally designed purely for speech. However, distance is unlimited because the modem signal is amplified as it travels through the network. PC modems only operate on PSTN whereas data-centre modems can be used for permanent connections (leased lines).

Modems:

SPEED	★	0 - 33.6 k
DISTANCE	★★★★★	Unlimited
QUICK INSTALL	★	15 - 30 mn

Fig. 3.30

Baseband modems -offer greater distances than line drivers but are more complex and therefore expensive. A baseband modem uses digital signalling technologies instead (FSK, 2B1Q, HDB3, HDSL, etc.). This enables extra distance for dedicated connections.

Baseband Modems:

SPEED	★★★★★	0 - 2000 k
DISTANCE	★★★	0 - 30 km
QUICK INSTALL	★★★	10 - 20 mn

Fig. 3.31

Null modem is a communication method to directly connect two DTEs (computer, terminal, printer, etc.) using an RS-232 serial cable. The name stems from the historical use of RS-232 cables to connect two teleprinter devices to two modems in order to communicate with one another; null modem communication refers to using a crossed-over RS-232 cable to connect the teleprinters directly to one another without the modems.

The RS-232 standard is asymmetric as to the definitions of the two ends of the communications link, assuming that one end is a DTE and the other is a DCE, e.g. a modem. With a null modem connection the transmit and receive lines are crosslinked. Depending on the purpose, sometimes also one or more handshake lines are crosslinked. Several wiring layouts are in use because the null modem connection is not covered by the RS-232 standard.

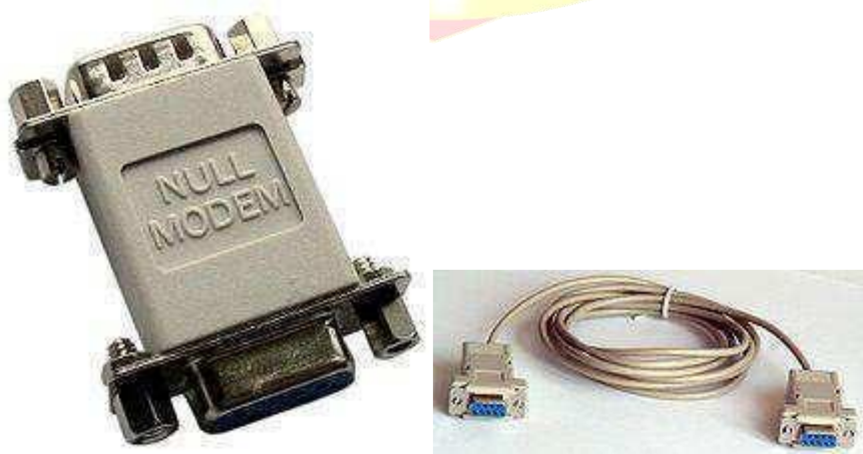


Fig. 3.32

REPEATERS

In telecommunications, a repeater is an electronic device that receives a signal and retransmits it. Repeaters are used to extend transmissions so that the signal can cover longer distances or be received on the other side of an obstruction. Some types of repeaters broadcast an identical signal, but alter its method of transmission, for example, on another frequency or baud rate. There are several different types of repeaters; a telephone repeater is an amplifier in a telephone line, an optical repeater is an optoelectronic circuit that amplifies the light beam in an optical fiber cable; and a radio repeater is a radio receiver and transmitter that retransmits a radio signal. A broadcast relay station is a repeater used in broadcast radio and television.

When an information-bearing signal passes through a communication channel, it is progressively degraded due to loss of power. For example, when a telephone call passes through a wire telephone line, some of the power in the electric current which represents the audio signal is dissipated as heat in the resistance of the copper wire. The longer the wire is, the more power is lost, and the smaller the amplitude of the signal at the far end. So with a long enough wire the call will not be audible at the other end. Similarly, the farther from a radio station a receiver is, the weaker the radio signal, and the poorer the reception. A repeater is an electronic device in a communication channel that increases the power of a signal and retransmits it, allowing it to travel further. Since it amplifies the signal, it requires a source of electric power.

The term "repeater" originated with telegraphy in the 19th century, and referred to an electromechanical device (a relay) used to regenerate telegraph signals. Use of the term has continued in telephony and data communications.

In computer networking, because repeaters work with the actual physical signal, and do not attempt to interpret the data being transmitted, they operate on the physical layer, the first layer of the OSI model.

Fig. 3.33

Repeaters can be divided into two types depending on the type of data they handle:

Analog repeater
This type is used in channels that transmit data in the form of an analog signal in which the voltage or current is proportional to the amplitude of the signal, as in an audio signal. They are also used in trunklines that transmit multiple signals using frequency division multiplexing (FDM). Analog repeaters are composed of a linear amplifier, and may include electronic filters to compensate for frequency and phase distortion in the line.

Digital repeater

The digipeater is used in channels that transmit data by binary digital signals, in which the data is in the form of pulses with only two possible values, representing the binary digits 1 and 0. A digital repeater amplifies the signal, and it also may retime, resynchronize, and reshape the pulses. A repeater that performs the retiming or resynchronizing functions may be called a regenerator.

Bridges

A bridge is a type of computer network device that provides interconnection with other bridge networks that use the same protocol. Bridge devices work at the data link layer of the Open System Interconnect (OSI) model, connecting two different networks together and providing communication between them. Bridges are similar to repeaters and hubs in that they broadcast data to every node. However, bridges maintain the media access control (MAC) address table as soon as they discover new segments, so subsequent transmissions are sent to only to the desired recipient. Bridges are also known as Layer 2 switches.

A network bridge device is primarily used in local area networks because they can potentially flood and clog a large network thanks to their ability to broadcast data to all the nodes if they don't know the destination node's MAC address.

A bridge uses a database to ascertain where to pass, transmit or discard the data frame.

If the frame received by the bridge is meant for a segment that resides on the same host network, it will pass the frame to that node and the receiving bridge will then discard it.

If the bridge receives a frame whose node MAC address is of the connected network, it will forward the frame toward it.

A bridge connecting two LAN segments

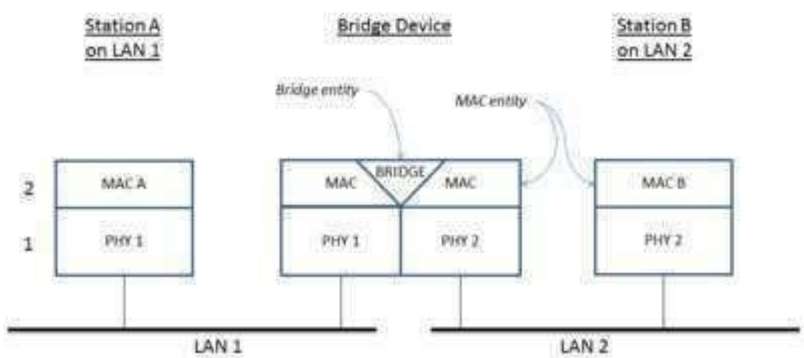


Fig. 3.34

A simple bridge connects two network segments, typically by operating transparently and deciding on a frame-by-frame basis whether or not to forward from one network to the other. A store and forward technique is typically used so, during forwarding, the frame integrity is verified on the source network and CSMA/CD delays are accommodated on the destination network. Contrary to repeaters that simply extend the maximum span of a segment, bridges only forward frames that are required to cross the bridge. Additionally, bridges reduce collisions by partitioning the collision domain.

A multiport bridge connects multiple networks and operates transparently to decide on a frame-by-frame basis whether and where to forward traffic. Like the simple bridge, a multiport bridge typically uses store and forward operation. The multiport bridge function serves as the basis for network switches.

A transparent bridge uses a forwarding database to send frames across network segments. The forwarding database starts empty - entries in the database are built as the bridge receives frames. If an address entry is not found in the forwarding database, the frame is flooded to all other ports of the bridge, flooding the frame to all segments except the one from which it was received. By means of these flooded frames, the destination network will respond and a forwarding database entry will be created.

In the context of a two-port bridge, one can think of the forwarding database as a filtering database. A bridge reads a frame's destination address and decides to either forward or filter. If the bridge determines that the destination node is on another segment on the network, it forwards (retransmits) the frame to that segment. If the destination address belongs to the same segment as the source address, the bridge filters (discards) the frame. As nodes transmit data through the bridge, the bridge establishes a filtering database of known MAC addresses and their locations on the network. The bridge uses its filtering database to determine whether a frame should be forwarded or filtered.

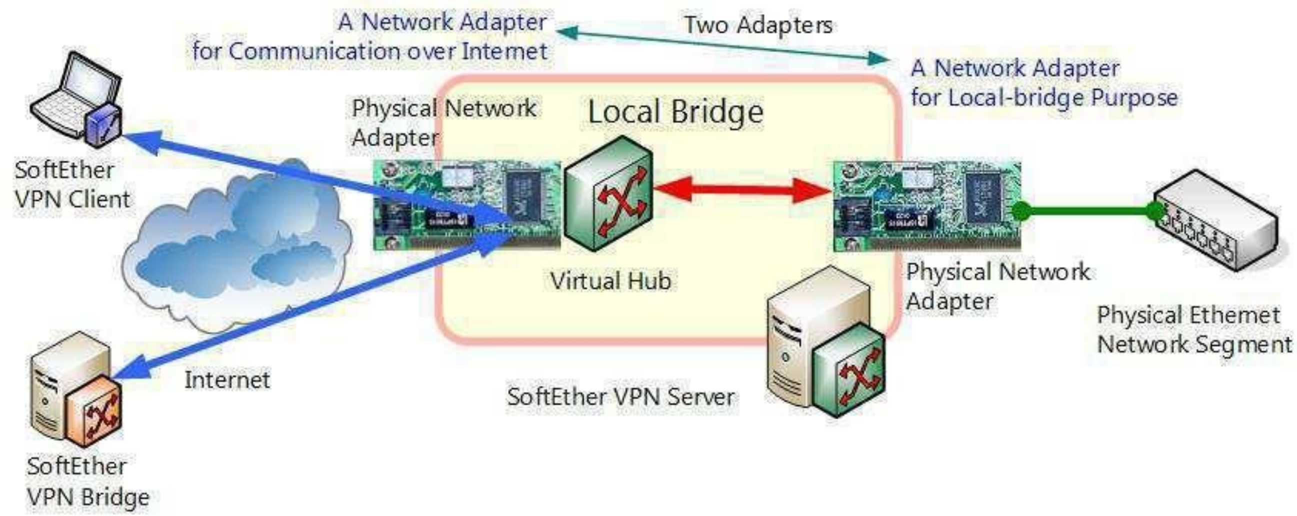


Fig. 3.35

Two & Three Layer Switches

LAN switching is a form of packet switching used in local area networks (LAN). Switching technologies are crucial to network design, as they allow traffic to be sent only where it is needed in most cases, using fast, hardware-based methods. LAN switching uses different kinds of network switches. A standard switch is known as a layer 2 switch and is commonly found in nearly any LAN.

Layer 2 switching uses the media access control address (MAC address) from the host's network interface cards (NICs) to decide where to forward frames. Layer 2 switching is hardware-based, which means switches use application-specific integrated circuit (ASICs) to build and maintain filter tables (also known as MAC address tables or CAM tables). One way to think of a layer 2 switch is as multiport bridge.

Layer 2 switching provides the following

1. Hardware-based bridging (MAC)
2. Wire speed / non-blocking forwarding
3. Low latency

Layer 2 switching is highly efficient because there is no modification to the data packet and the frame, encapsulation of the packet changes only when the data packet is passing through dissimilar media (such as from Ethernet to FDDI). Layer 2 switching is used for work group connectivity and network segmentation (breaking up collision domains). This allows a flatter network design with more network segments than traditional networks joined by repeater hubs and routers. Layer 2 switching has helped develop new components in the network infrastructure.

- Server farms — Servers need no longer be distributed to physical locations because virtual LANs can be created to create broadcast domains and network proximity in a switched internetwork. This means that all servers can be placed in a central location, yet a certain server can still be part of a workgroup in a remote branch, for example.
- Intranets — Allows organization-wide client/server communications based on a Web technology.

These new technologies allow more data to flow off from local subnets and onto a routed network, where a router's performance can become the bottleneck.

Limitations

Layer 2 switches have the same limitations as bridge networks. Bridges are good if a network is designed by the 80/20 rule: users spend 80 percent of their time on their local segment.

Bridged networks break up collision domains, but the network remains one large broadcast domain. Similarly, layer 2 switches (bridges) cannot break up broadcast domains, which can cause performance issues and limits the size of your network. Broadcast and multicasts, along with the slow convergence of spanning tree, can cause major problems as the network grows. Because of these problems, layer 2 switches cannot completely replace routers in the internet work.

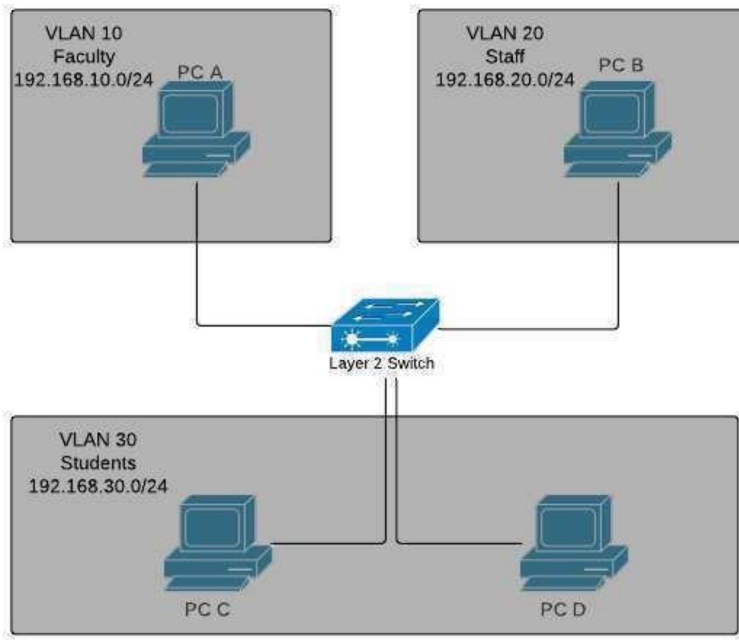


Fig. 3.36

Fig. 3.37

Layer 3 switching

Layer 3 switching is solely based on (destination) IP address stored in the header of IP datagram (see layer 4 switching later on this page for the difference). The difference between a layer 3 switch and a router is the way the device is making the routing decision. Traditionally, routers use microprocessors to make forwarding decisions in software, while the switch performs only hardware-based packet switching (by specialized ASIC with the help of content-addressable memory). However, some traditional routers can have advanced hardware functions as well in some of the higher-end models.

The main advantage of layer 3 switches is the potential for lower network latency as a packet can be routed without making extra network hops to a router. For example, connecting two distinct segments (e.g. VLANs) with a router to a standard layer 2 switch requires passing the frame to the switch (first L2 hop), then to the router (second L2 hop) where the packet inside the frame is routed (L3 hop) and then passed back to the switch (third L2 hop). A layer 3 switch accomplishes the same task without the need for a router (and therefore additional hops) by making the routing decision itself, i.e. the packet is routed to another subnet and switched to the destination network port simultaneously.

Because many layer 3 switches offer the same functionality as traditional routers they can be used as cheaper, lower latency replacements in some networks. Layer 3 switches can perform the following actions that can also be performed by routers:

1. determine paths based on logical addressing
2. run layer 3 checksums (on header only)
3. use Time to Live (TTL)
4. process and respond to any option information
5. update Simple Network Management Protocol (SNMP) managers with Management Information Base (MIB) information
6. provide Security

The benefits of layer 3 switching include the following:

1. fast hardware-based packet forwarding
2. high-performance packet switching
3. high-speed scalability
4. low latency
5. lower per-port cost
6. flow accounting
7. Quality of service (QoS)

The switching algorithm is relatively simple and is the same for most of the routed protocols: a host would like to send a packet to a host on another network. Having acquired a router's address by some means, the source host sends the packet directly to that router's physical (MAC) address. The protocol (network layer) address is that of the destination host.

The router examines the packet's destination protocol address and determines whether it knows how to forward the packet or not. If the router does not know how to forward the packet, it typically drops the packet. If it knows how to forward packet, it changes the destination physical address to that of the next hop router and transmits the packet.

The next hop may be the destination or the next router, which executes the same switching process. As the packet moves through the internetwork, its physical address changes, but its protocol address remains same.

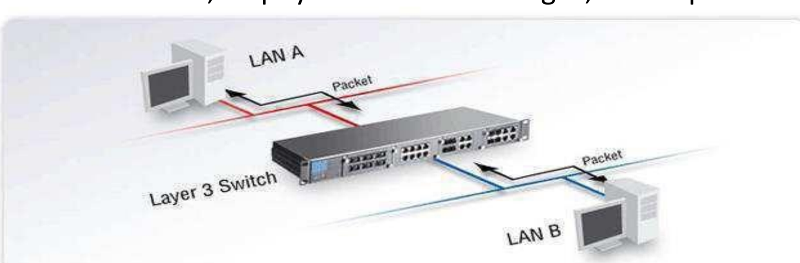


Fig. 3.38

Fig. 3.39

IEEE has developed hierarchical terminology that is useful in describing this process. Network devices without the capability to forward packets between subnetworks are called end systems (ESs, singular ES), whereas network devices with these capabilities are called intermediate systems (ISs). ISs are further divided into those that communicate only within their routing domain (Intradomain IS) and those that communicate both within and between routing domains (Interdomains IS). A routing domain is generally considered as portion of an internetwork under common administrative authority and is regulated by a particular set of administrative guidelines. Routing domains are also called autonomous systems.

Gateway

The most common gateway is a router that connects a home or enterprise network to the internet. In most IP-based networks, the only traffic that doesn't go through at least one gateway is traffic flowing among nodes on the same local area network (LAN) segment - for example, computers connected to the same switch.
Gateways can take several forms and perform a variety of tasks. These include:

Web application firewall - filters traffic to and from a web server and look at application-layer data.

API, SOA or XML gateway - manages traffic flowing into and out of a service, microservices-oriented architecture or an XML-based web service.

IoT gateway - aggregates sensor data, translates between sensor protocols, processes sensor data before sending it onward and more.

Cloud storage gateway - translates storage requests with various cloud storage service API calls.

Media gateway - converts data from the format required for one type of network to the format required for another.

Amazon API Gateway - allows a developer to connect non-AWS applications to AWS back-end resources.

VoIP trunk gateway - facilitates the use of plain old telephone service (POTS) equipment, such as landline phones and fax machines, with a voice over IP (VoIP) network.

Email security gateway - prevents the transmission of emails that break company policy or will transfer information with malicious intent.

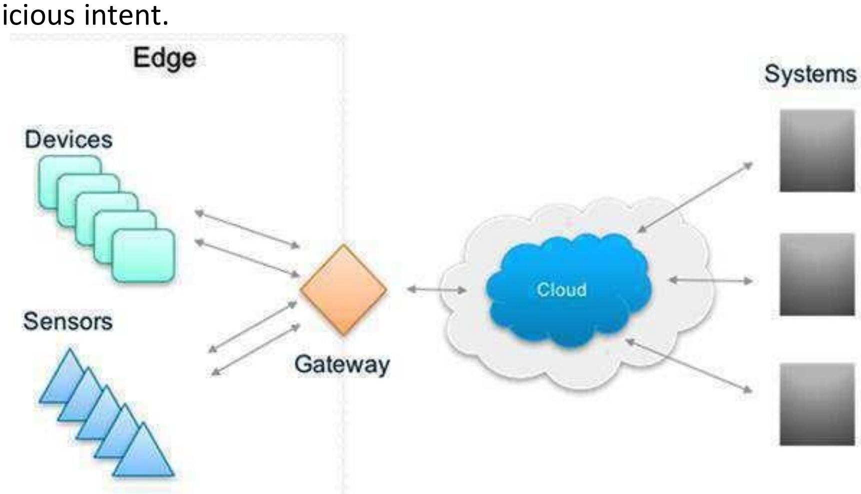


Fig. 3.40

Fig. 3.41

Study of various Topology

Network topology means the physical or logical layout of a network in which define how the different nodes are placed and interconnected with each other and also describe how the data is transferred between these nodes.

The Star Topology

In this topology each of the devices and computers on a network connect to a central hub / switch. A major disadvantage of this type of network topology is that if the central hub fails, all computers connected to that hub would be disconnected. All information on a star network first passes through the hub or switch before continuing to its destination. It also acts as a repeater for the data flow. Mostly we use twisted pair cable to connected all the computer with central device but we may also use coaxial or fiber optical cable.

Advantages of Star Topology

1. It is easy to modify and can add new computer or remove without disturbing the rest of the network.
2. Single computer backbones do not necessary backbone the whole network.
3. Several cable type can be used in same network with a hub
4. Easy to install and wire
5. Easy tom detect faults and remove parts

Disadvantages of Star Topology

1. Requires more cable length then a linear topology
2. If the hub or connector fail, nodes attach are disturb.
3. More expensive then linear bus topology because of the cast of the concentration.

Ring Topology

In Ring topology all the devices or computer are connected to each other in a circular shape. All the data which will be send move around the ring until it reaches its final destination.

Advantages of Ring Topology

•As every computer is given is equal access to the token. No one computer can normalize the network.

•If a terminal becomes effective, it can be by pass without affecting the network.

•If a terminal working as the central computer. Any other node can be made by central computer and the network keep on the working

Disadvantage of Ring Topology

•Failure of the one computer of the ring can be effective the whole network.

•It is difficult to trouble shoot a ring network.
•Adding and removing computer disturb the network

Token-ring

In Token Ring topology all the computer are organized in a ring topology. Data passes sequentially between nodes on the network until it returns to the source station. To prevent traffic and collision, a token is used to ensure that only one computer on the line is used at a time. A token ring LAN is physically wired as a star topology but configured as a ring topology.

The Bus Topology

In This topology all the computer computer and devices are connected to a single cable. This is typically use in a small networks and takes advantage of using less cable. Their main disadvantage is that if any segment of the network fails, all transmissions do as well.

Advantages of bus topology

•The bus is simple, reliable in a very small network, easy to use and east to understand
•The bus requires the last amount of cable to connect the computer together and therefore less expensive than other cabling arrangement
•It is easy to extend a bus. Cable can be joint into one longer cable allowing more computers to attach

Disadvantages of Bus Topology

•Heavy network traffic can slow a bus considerably.
•It is difficult be easy to troubleshoot a bus. If there is an error in the system it cannot be easily to detect.
•The entire network shuts down if there is a break with main cable.

Tree topology

in tree topology more then two hub are connected each other this topology is collection of linear bus and star topology. The Each star network is a local area network with central computer or server and all the node direct ally link to this server and the central computers or server of the star networks are connected to a main cable called the bus.

Advantages of Tree topology

1. Point to point wiring for individual segments.
2. Supported by several hardware and software venders.

Disadvantages of Tree topology

1. Overall length of each segment is limited by the type of cabling used.
2. If the backbone line breaks the entire segment goes down.

•More difficult to configure and wire than other topologies

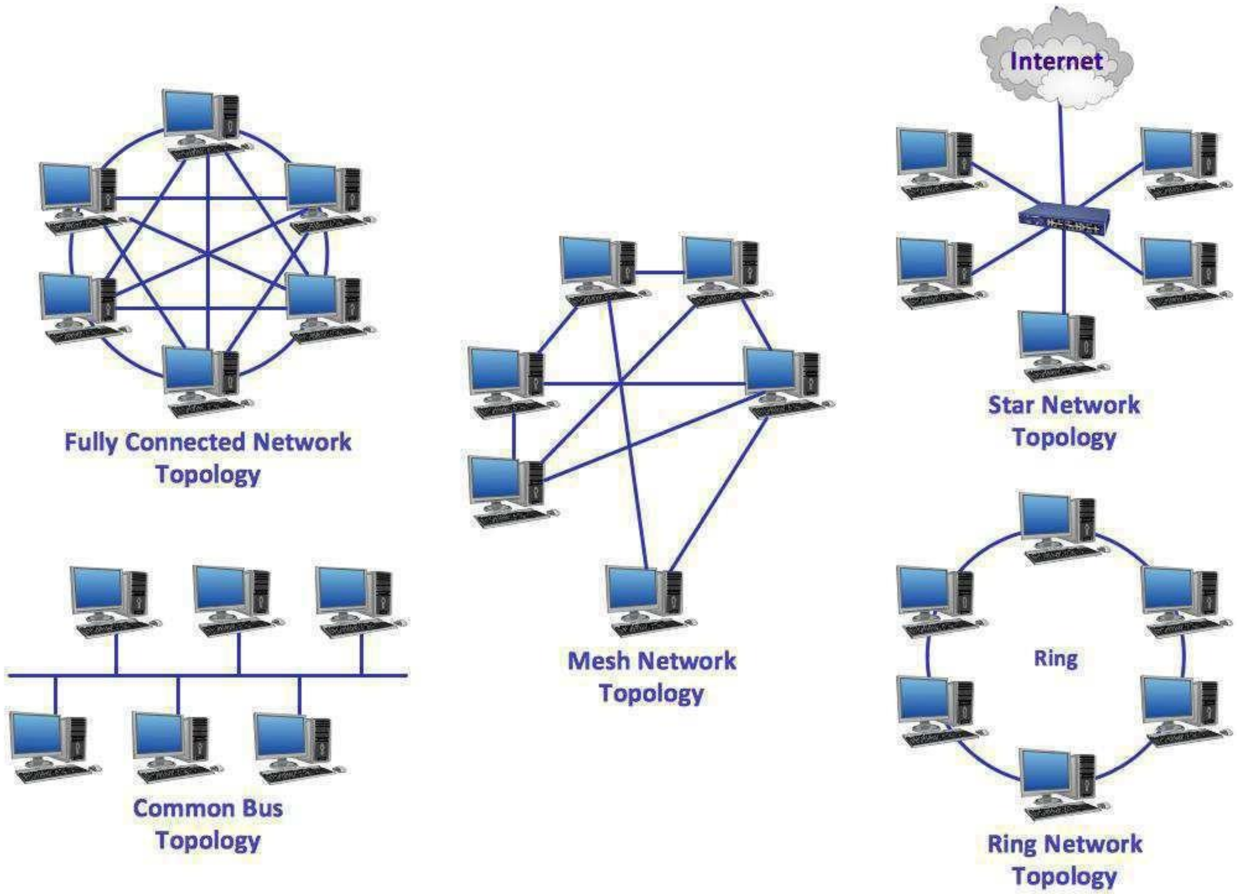


Fig. 3.42

Introduction to Queing Theory

Queueing theory is the mathematical study of waiting lines, or queues. A queueing model is constructed so that queue lengths and waiting time can be predicted. Queueing theory is generally considered a branch of operations research because the results are often used when making business decisions about the resources needed to provide a service.

Queueing theory has its origins in research by AgnerKrarupErlang when he created models to describe the Copenhagen telephone exchange. The ideas have since seen applications including telecommunication, traffic engineering, computing and, particularly in industrial engineering, in the design of factories, shops, offices and hospitals, as well as in project management.

Single queueing nodes are usually described using Kendall's notation in the form A/S/C where A describes the time between arrivals to the queue, S the size of jobs and C the number of servers at the node. Many theorems in queueing theory can be proved by reducing queues to mathematical systems known as Markov chains, first described by Andrey Markov in his 1906 paper.

Various scheduling policies can be used at queuing nodes:

First in first out

This principle states that customers are served one at a time and that the customer that has been waiting the longest is served first.

Last in first out

This principle also serves customers one at a time, but the customer with the shortest waiting time will be served first. Also known as a stack.

Processor sharing

Service capacity is shared equally between customers.

Priority

Customers with high priority are served first. Priority queues can be of two types, non-preemptive (where a job in service cannot be interrupted) and preemptive (where a job in service can be interrupted by a higher-priority job). No work is lost in either model.

Shortest job first

The next job to be served is the one with the smallest size

Preemptive shortest job first

The next job to be served is the one with the original smallest size

Shortest remaining processing time

The next job to serve is the one with the smallest remaining processing requirement.

Service facility

Single server: customers line up and there is only one server

Parallel servers: customers line up and there are several servers

Tandem queue: there are many counters and customers can decide going where to queue Customer's behavior of waiting

Balking: customers deciding not to join the queue if it is too long

Jockeying: customers switch between queues if they think they will get served faster by doing so

Reneging: customers leave the queue if they have waited too long for service

AgnerKrarupErlang, a Danish engineer who worked for the Copenhagen Telephone Exchange, published the first paper on what would now be called queueing theory in 1909. He modeled the number of telephone calls arriving at an exchange by a Poisson process and solved the M/D/1 queue in 1917 and M/D/k queueing model in 1920. In Kendall's notation:

M stands for Markov or memoryless and means arrivals occur according to a Poisson processD stands for deterministic and means jobs arriving at the queue require a fixed amount of servicek describes the number of servers at the queueing node (k = 1, 2,...). If there are more jobs at the node than there are servers then jobs will queue and wait for service

The M/M/1 queue is a simple model where a single server serves jobs that arrive according to a Poisson process and have exponentially distributed service requirements. In an M/G/1 queue the G stands for general and indicates an arbitrary probability distribution. The M/G/1 model was solved by Felix Pollaczek in 1930, a solution later recast in probabilistic terms by AleksandrKhinchin and now known as the Pollaczek–Khinchine formula.

After the 1940s queueing theory became an area of research interest to mathematicians. In 1953 David George Kendall solved the GI/M/k queue and introduced the modern notation for queues, now known as Kendall's notation. In 1957 Pollaczek studied the GI/G/1 using an integral equation. John Kingman gave a formula for the mean waiting time in a G/G/1 queue: Kingman's formula.

The matrix geometric method and matrix analytic methods have allowed queues with phase-type distributed inter-arrival and service time distributions to be considered.

Problems such as performance metrics for the M/G/k queue remain an open problem.

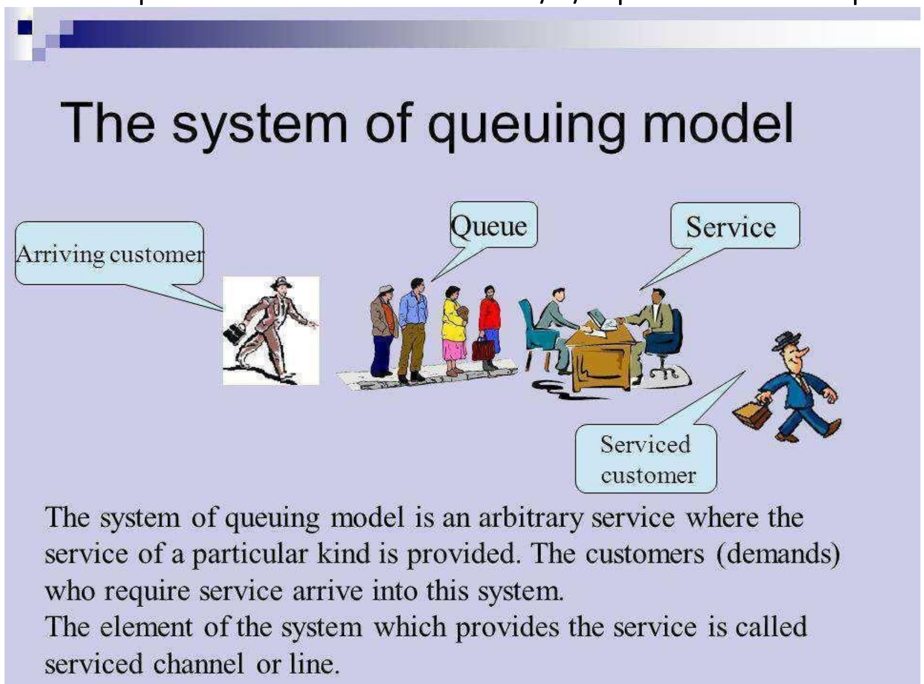


Fig. 3.43

UNIT-IV

Transmission Line Characteristics

INTRODUCTION: Digital systems generally require the transmission of digital signals to and from other elements of the system. The component wavelengths of the digital signals will usually be shorter than the electrical length of the cable used to connect the subsystems together and, therefore, the cables should be treated as a transmissions line. In addition, the digital signal is usually exposed to hostile electrical noise sources which will require more noise immunity than required in the individual subsystems environment. The requirements for transmission line techniques and noise immunity are recognized by the designers of subsystems and systems, but the solutions used vary considerably. Two widely used example methods of the solution are shown. The two methods illustrated use unbalanced and balanced circuit techniques. This application note will delineate the characteristics of digital signals in transmission lines and characteristics of the line that effect the quality, and will compare the unbalanced and balanced circuits performance in digital systems.

NOISE The cables used to transmit digital signals external to a subsystem and in route between the subsystem, are exposed to external electromagnetic noise caused by switching transients from actuating devices of neighboring control systems. Also external to a specific subsystem, another subsystem may have a ground problem which will induce noise on the system, as indicated in Figure 2. The signals in adjacent wires inside a cable may induce electromagnetic noise on other wires in the cable. The induced electromagnetic noise is worse when a line terminated at one end of the cable is near to a driver at the same end, as shown in Figure 3. Some noise may be induced from relay circuits which have very large transient voltage swings compared to the digital signals in the same cable. Another source of induced noise is current in the common ground wire or wires in the cable.

DISTORTION The objective is the transmission and recovery of digital intelligence between subsystems, and to this end, the characteristics of the data recovered must resemble the data transmitted. In Figure 4 there is a difference in the pulse width of the data and the timing signal transmitted, and the corresponding signal received. In addition there is a further difference in the signal when the data is "AND"ed with the timing signal. The distortion of the signal occurred in the transmission line and in the line driver and receiver.
A primary cause of distortion is the effect the transmission line has on the rise time of the transmitted data. what happens to a voltage step from the driver as it travels down the line. The rise time of the signal increases as the signal travels down the line. This effect will tend to affect the timing of the recovered signal.

The velocity factor (VF) also called wave propagation speed or velocity of propagation (VoP), of a transmission medium is the ratio of the speed at which a wavefront (of an acoustic signal, for example, or an electromagnetic signal, a radio signal, a light pulse in a fibre channel or a change of the electrical voltage on a copper wire) passes through the medium, to the speed of light in a vacuum. For optical signals, the velocity factor is the reciprocal of the refractive index.

The speed of radio signals in a vacuum, for example, is the speed of light, and so the velocity factor of a radio wave in a vacuum is unity, or 100%. In electrical cables, the velocity factor mainly depends on the insulating material (see table below).
The use of the terms velocity of propagation and wave propagation speed to mean a ratio of speeds is confined to the computer networking and cable industries. In a general science and engineering context, these terms would be understood to mean a true speed or velocity in units of distance per time, while velocity factor is used for the ratio.

CROSS TALK

In electronics, crosstalk is any phenomenon by which a signal transmitted on one circuit or channel of a transmission system creates an undesired effect in another circuit or channel. Crosstalk is usually caused by undesired capacitive, inductive, or conductive coupling from one circuit or channel to another.
Crosstalk is a significant issue in structured cabling, audio electronics, integrated circuit design, wireless communication and other communications systems.
In structured cabling, crosstalk can refer to electromagnetic interference from one unshielded twisted pair to another twisted pair, normally running in parallel.

Near end crosstalk (NEXT)

NEXT is a measure of the ability of cabling to reject crosstalk. Interference between two pairs in a cable is measured at the same end of the cable as the interfering transmitter. Crosstalk is undesirable. In crosstalk, the signals traveling through adjacent pairs of wire in twisted-pair cabling interfere with each other. The pair causing the interference is called the “disturbing pair,” while the pair experiencing the interference is the “disturbed pair.” Channel NEXT is the NEXT value measured between one wire pair and another in the same cable; NEXT is measured at both ends of the wire. The NEXT value for a given cable type is generally expressed in decibels per feet or decibels per 1000 feet. NEXT value varies with the frequency of transmission. The higher the NEXT value, the greater the cable’s ability to reject crosstalk at its local connection. Generally specifications for cabling (such as CAT 5) include the minimum NEXT values.

Power sum near end crosstalk (PSNEXT)

PSNEXT is a NEXT measurement which includes the sum of crosstalk contributions of all adjacent pairs. It is the algebraic sum of near-end crosstalk (NEXT) of three wire pairs as they affect the fourth pair in a four-pair cable (e.g., Category 6 cable). The specification was developed to directly address the effect of transmissions on multiple adjacent pairs on the pair being tested and is relevant to all connecting hardware and associated communications cables. Cabling bandwidths in excess of 100 MHz (Category 5 cable bandwidth) make consideration of PSNEXT more important. Gigabit Ethernet through Cat-6 uses all four wire pairs simultaneously and bidirectionally. The additional wire pair usage and growing bandwidth increase the need to keep NEXT in check.
PSNEXT is a way of measuring NEXT in the ends of cables due to their close proximity. The (cited) SMP white paper states that the testing process for PSNEXT consists of measuring all pair-to-pair crosstalk combinations and then summing all of the values for each pair.

Far end crosstalk (FEXT)

Interference between two pairs of a cable measured at the other end of the cable with respect to the interfering transmitter.

Equal level far end crosstalk (ELFEXT)

An FEXT measurement with attenuation compensation.

Alien crosstalk (AXT)

Interference caused by other cables routed close to the cable of interest.

Transmission Mediums in Data Communication

Data is represented by computers and other telecommunication devices using signals. Signals are transmitted in the form of electromagnetic energy from one device to another. Electromagnetic signals travel through vacuum, air or other transmission mediums to travel between one point to another(from source to receiver).

Electromagnetic energy (includes electrical and magnetic fields) includes power, voice, visible light, radio waves, ultraviolet light, gamma rays etc.

Transmission medium is the means through which we send our data from one place to another. The first layer (physical layer) of Communication Networks OSI Seven layer model is dedicated to the transmission media, we will study the OSI Model later.

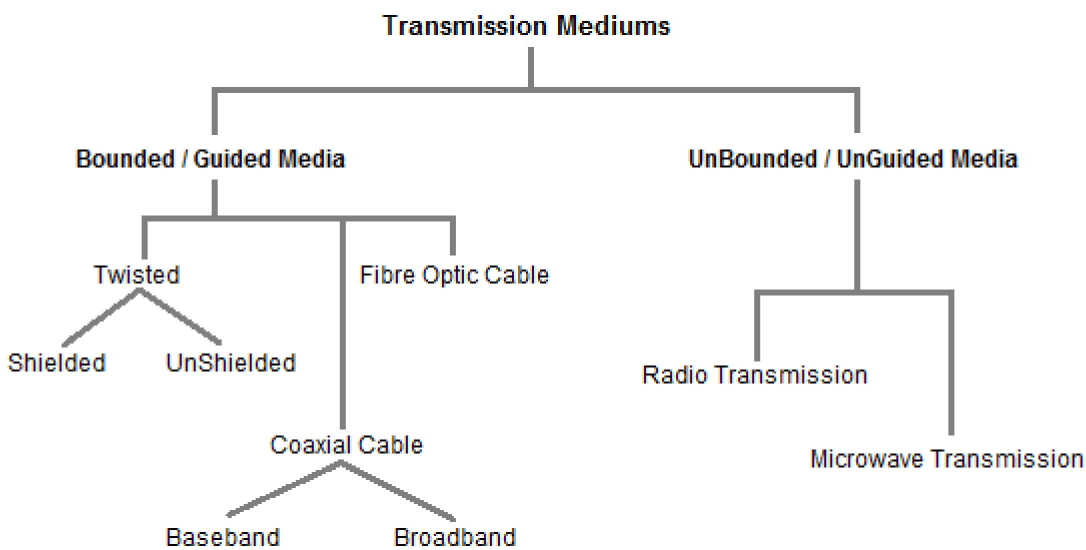


Fig. 4.1

Factors to be considered while choosing Transmission Medium

Transmission Rate

Cost and Ease of Installation

Resistance to Environmental Conditions

Distances

Bounded/Guided Transmission Media
It is the transmission media in which signals are confined to a specific path using wire or cable. The types of Bounded/ Guided are discussed below.

Twisted Pair Cable

This cable is the most commonly used and is cheaper than others. It is lightweight, cheap, can be installed easily, and they support many different types of network. Some important points :
Its frequency range is 0 to 3.5 kHz.
Typical attenuation is 0.2 dB/Km @ 1kHz.
Typical delay is 50 µs/km.
Repeater spacing is 2km.
Twisted Pair is of two types :
Unshielded Twisted Pair (UTP)
Shielded Twisted Pair (STP)

Unshielded Twisted Pair Cable
It is the most common type of telecommunication when compared with Shielded Twisted Pair Cable which consists of two conductors usually copper, each with its own colour plastic insulator. Identification is the reason behind coloured plastic insulation.

- Installation is easy
- Flexible
- Cheap
- It has high speed capacity,
- 100 meter limit
- Higher grades of UTP are used in LAN technologies like Ethernet.

It consists of two insulating copper wires (1mm thick). The wires are twisted together in a helical form to reduce electrical interference from similar pair.

Disadvantages :
Bandwidth is low when compared with Coaxial Cable
Provides less protection from interference.

Shielded Twisted Pair Cable

This cable has a metal foil or braided-mesh covering which encases each pair of insulated conductors. Electromagnetic noise penetration is prevented by metal casing. Shielding also eliminates crosstalk .

It has same attenuation as unshielded twisted pair. It is faster the unshielded and coaxial cable. It is more expensive than coaxial and unshielded twisted pair.

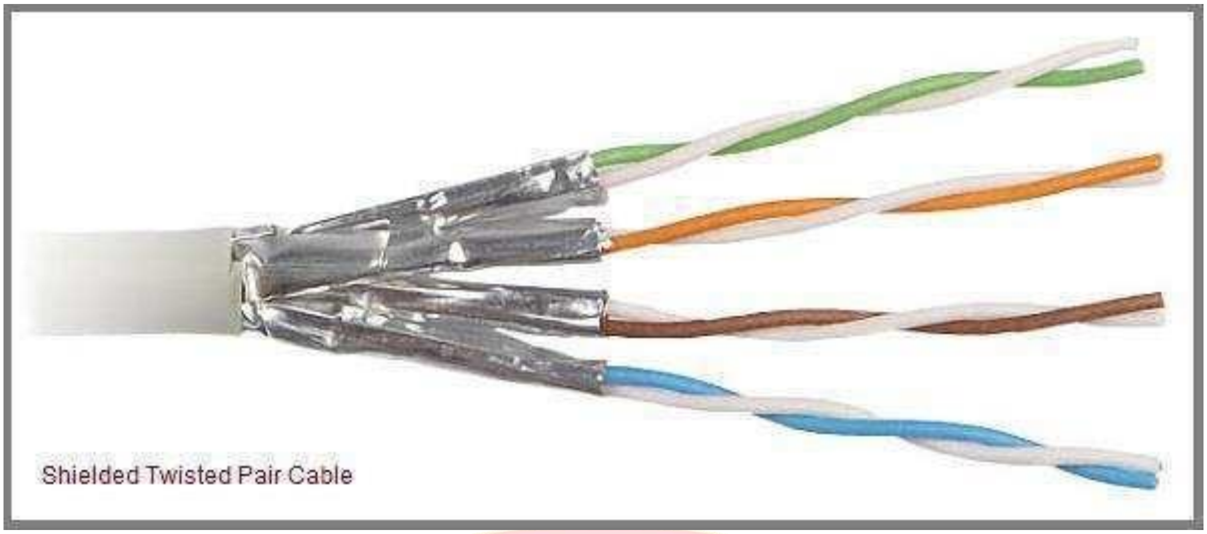


Fig. 4.2

Advantages :

- Easy to install
- Performance is adequate
- Can be used for Analog or Digital transmission
- Increases the signalling rate
- Higher capacity than unshielded twisted pair
- Eliminates crosstalk

Disadvantages :

- Difficult to manufacture
- Heavy

Coaxial Cable

Coaxial is called by this name because it contains two conductors that are parallel to each other. Copper is used in this as centre conductor which can be a solid wire or a standard one. It is surrounded by PVC installation, a sheath which is encased in an outer conductor of metal foil, barid or both.

Outer metallic wrapping is used as a shield against noise and as the second conductor which completes the circuit. The outer conductor is also encased in an insulating sheath. The outermost part is the plastic cover which protects the whole cable.

Here the most common coaxial standards.

- 50-Ohm RG-7 or RG-11 : used with thick Ethernet.
- 50-Ohm RG-58 : used with thin Ethernet
- 75-Ohm RG-59 : used with cable television
- 93-Ohm RG-62 : used with ARCNET.

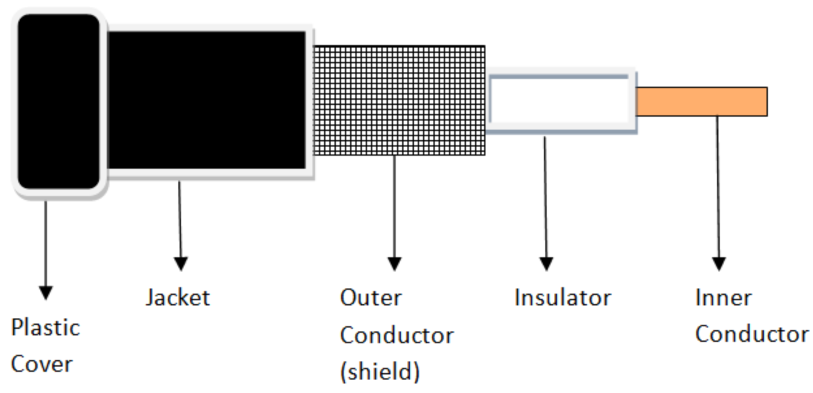


Fig. 4.3

There are two types of Coaxial cables :

BaseBand

This is a 50 ohm (Ω) coaxial cable which is used for digital transmission. It is mostly used for LAN's. Baseband transmits a single signal at a time with very high speed. The major drawback is that it needs amplification after every 1000 feet.

BroadBand

This uses analog transmission on standard cable television cabling. It transmits several simultaneous signal using different frequencies. It covers large area when compared with Baseband Coaxial Cable.

Advantages :

- Bandwidth is high
- Used in long distance telephone lines.
- Transmits digital signals at a very high rate of 10Mbps.
- Much higher noise immunity
- Data transmission without distortion.
- The can span to longer distance at higher speeds as they have better shielding when compared to twisted pair cable

Disadvantages :

- Single cable failure can fail the entire network.
- Difficult to install and expensive when compared with twisted pair.
- If the shield is imperfect, it can lead to grounded loop.

Optical Fiber

An optical fiber or optical fibre is a flexible, transparent fiber made by drawing glass (silica) or plastic to a diameter slightly thicker than that of a human hair. Optical fibers are used most often as a means to transmit light between the two ends of the fiber and find wide usage in fiber-optic communications, where they permit transmission over longer distances and at higher bandwidths (data rates) than wire cables. Fibers are used instead of metal wires because signals travel along them with less loss; in addition, fibers are immune to electromagnetic interference, a problem from which metal wires suffer excessively.Fibers are also used for illumination, and are wrapped in bundles so that they may be used to carry images, thus allowing viewing in confined spaces, as in the case of a fiberscope. Specially designed fibers are also used for a variety of other applications, some of them being fiber optic sensors and fiber lasers.

These are similar to coaxial cable. It uses electric signals to transmit data. At the centre is the glass core through which light propagates.

In multimode fibres, the core is 50microns, and In single mode fibres, the thickness is 8 to 10 microns.

The core in fiber optic cable is surrounded by glass cladding with lower index of refraction as compared to core to keep all the light in core. This is covered with a thin plastic jacket to protect the cladding. The fibers are grouped together in bundles protected by an outer shield.

Fiber optic cable has bandwidth more than **2 gbps (Gigabytes per Second)**

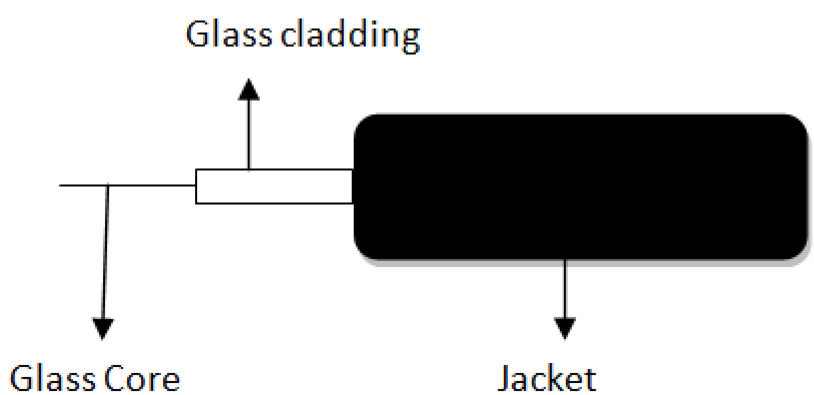


Fig. 4.4

Advantages :
Provides high quality transmission of signals at very high speed.
These are not affected by electromagnetic interference, so noise and distortion is very less.
Used for both analog and digital signals.

Disadvantages :
- It is expensive
- Difficult to install.
- Maintenance is expensive and difficult.
- Do not allow complete routing of light signals.

Physics and Velocity of Propagation of Light
Whereas the velocity of some particle is a quantity which is based on a fairly simple and unambiguous concept, the velocity of light (as of other wave phenomena) is a much more

sophisticated matter. There are different kinds of velocities, which are different conceptually and can (particularly for light propagation in media) have substantially different values:

1. The phase velocity is the velocity with which phase fronts propagate.
2. The group velocity determines the speed with which intensity maxima propagate (e.g. the peaks of pulses).
3. The velocity of information transport can differ from both phase and group velocity.

The velocity factor (VF), also called wave propagation speed or velocity of propagation of a transmission medium is the ratio of the speed at which a wave for example, or an electromagnetic signal, a radio signal, a light pulse in an optical fibre or a change of the electrical voltage on a copper wire) passes through the medium, to the speed of light in a vacuum. For optical signals, the velocity factor is the reciprocal of the refractive index.
The speed of radio signals in a vacuum, for example, is the speed of light, and so the velocity factor of a radio wave in a vacuum is unity, or 100%. In electrical cables, the velocity factor mainly depends on the insulating material .

The use of the terms velocity of propagation and wave propagation speed to mean a ratio of speeds is confined to the computer networking and cable industries. In a general science and engineering context, these terms would be understood to mean a true speed or velocity in units of distance per time, while velocity factor is used for the ratio.

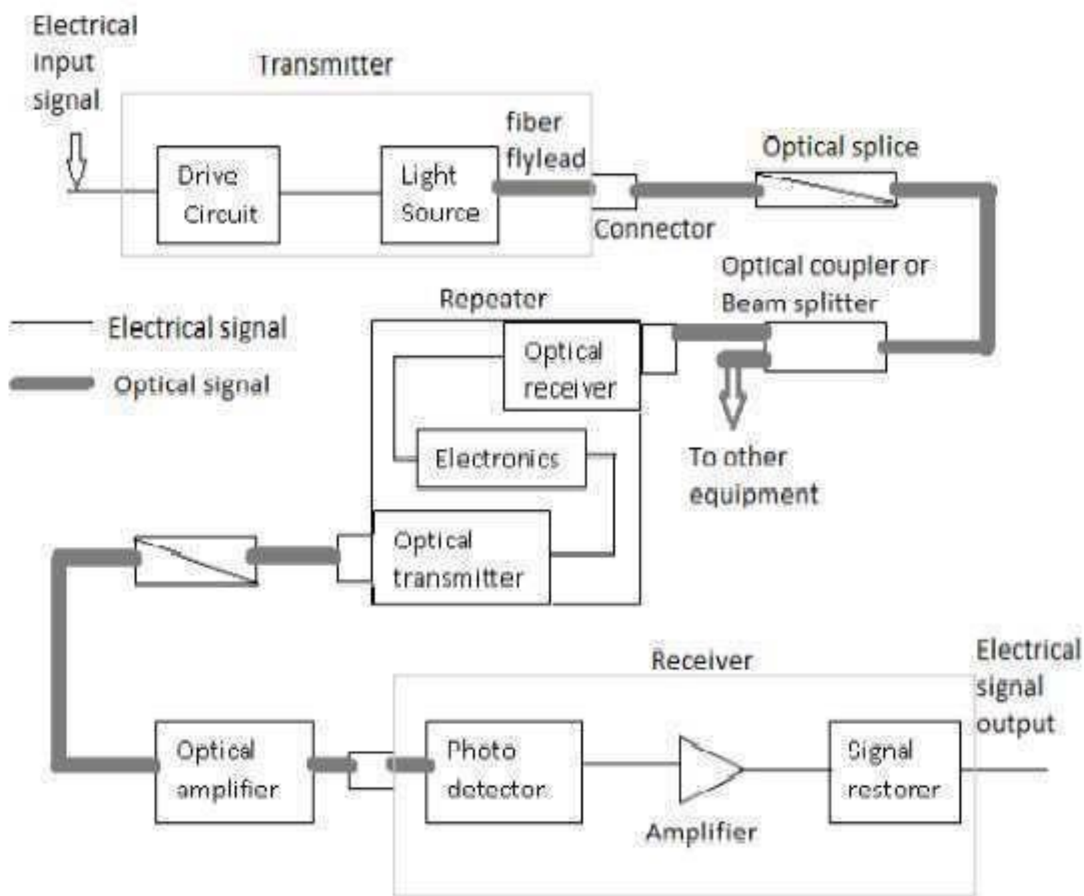


Fig. 4.5

The optical fiber consists of three main elements:

Transmitter: An electric signal is applied to the optical transmitter. The optical transmitter consists of driver circuit, light source and fiber flylead.

Driver circuit drives the light source.

Light source converts electrical signal to optical signal.

Fiber flylead is used to connect optical signal to optical fiber.

Transmission channel: It consists of a cable that provides mechanical and environmental protection to the optical fibers contained inside. Each optical fiber acts as an individual channel.

Optical splice is used to permanently join two individual optical fibers.

Optical connector is for temporary non-fixed joints between two individual optical fibers.

Optical coupler or splitter provides signal to other devices.

Repeater converts the optical signal into electrical signal using optical receiver and passes it to electronic circuit where it is reshaped and amplified as it gets attenuated and distorted with increasing distance because of scattering, absorption and dispersion in waveguides, and this signal is then again converted into optical signal by the optical transmitter.

Receiver: Optical signal is applied to the optical receiver. It consists of photo detector, amplifier and signal restorer.

Photo detector converts the optical signal to electrical signal.
Signal restorers and amplifiers are used to improve signal to noise ratio of the signal as there are chances of noise to be introduced in the signal due to the use of photo detectors.
For short distance communication only main elements are required.
Source- LED
Fiber- Multimode step index fiber
Detector- PIN detector
For long distance communication along with the main elements there is need for couplers, beam splitters, repeaters, optical amplifiers.
Source- LASER diode
Fiber- single mode fiber
Detector- Avalanche photo diode (APD)

Sources and qualities of light
Non-laser sources: Tungsten--Halogen Mercury Xenon Metal halid Light emitting diodes (LEDs) Monochromator Lasers: Gas, Helium-based , Diode , IR
Emission of light, (in the form of a photon) can take place either spontaneously or it can be stimulated by the presence of another photon of the right energy level.
For spontaneous or stimulated emission to occur, energy must be supplied to boost the electron from its low energy state to a higher energy state.
The energy can come from many sources: Heat (Incandescent light), Electrical Discharge (D2 , Hg, Na lamps), Electrical Current (LED, LD), Bioluminescence (Fire fly- luciferase enzyme)
OPTICAL SOURCES: Optical Source find applications in the area of medical, automotive, analytical equipments, communications and industry.

Types of Optical Source Tungsten, Deuterium, Mercury, Hollow Cathode Lamp Optical Source specifically suited to FO systems are: Light Emitting Diode (SLED, ELED, SLD) Laser Diode (DFB, DBR).

Optical Source Requirement for Performance (For Fiber Optics)
- Physical dimensions to suit the optical fiber
- Narrow radiation pattern (beam width)
- Linearity (output light power proportional to driving current)
- Ability to be directly modulated by varying driving current
- Fast response time
- Adequate output power into the fiber
- Narrow spectral width (or line width)
- Stability and efficiency
- Driving circuit issues
- Reliability and cost

Electromagnetic waves
EM waves are energy transported through space in the form of periodic disturbances of electric and magnetic fields.

EM waves travel through space at the same speed, c = 2.99792458 x 108 m/s, commonly known as the speed of light.
An EM wave is characterized by a frequency and a wavelength.
These two quantities are related to the speed of light by the equation speed of light = frequency x wavelength
The frequency (or wavelength) of an EM wave depends on its source.
There is a wide range of frequency encountered in our physical world, ranging from the low frequency of the electric waves generated by the power transmission lines to the very high frequency of the gamma rays originating from the atomic nuclei. This wide frequency range of electromagnetic waves constitute the Electromagnetic Spectrum.

Electromagnetic Spectrum
Visible: Small portion of the EMS that humans are sensitive to: blue (0.4-0.5 µm); green (0.5-0.6 µm); red (0.6-0.73 µm)
Infrared: Three logical zones: 1. Near IR: reflected, can be recorded on film emulsions (0.7 - 1.3 µm). 2. Mid infrared: reflected, can be detected using electro-optical sensors (1.3 - 3.0 µm). 3. Thermal infrared: emitted, can only be detected using electro-optical sensors (3.0 - 5.0 and 8 - 14 µm).
Microwave Radar sensors, wavelengths range from 1mm - 1m (K a, K u, X, C, S, L & P)

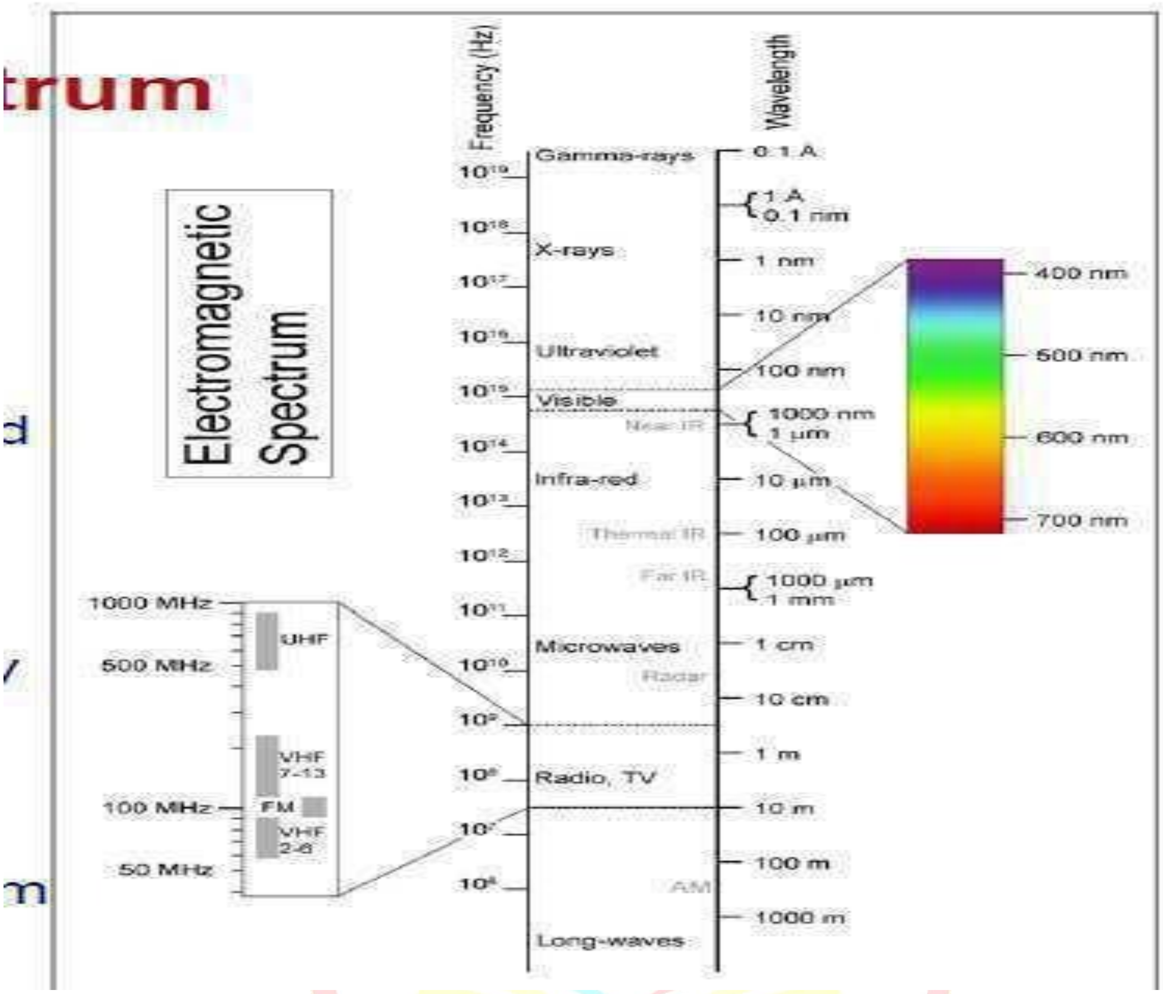


Fig. 4.6

Wavelengths of microwave

- Microwaves: 1 mm to 1 m wavelength.
- Further divided into different frequency bands:(1 GHz = 109 Hz)
- P band: 0.3 - 1 GHz (30 - 100 cm)
- L band: 1 - 2 GHz (15 - 30 cm)
- S band: 2 - 4 GHz (7.5 - 15 cm)
- C band: 4 - 8 GHz (3.8 - 7.5 cm)
- X band: 8 - 12.5 GHz (2.4 - 3.8 cm)
- Ku band: 12.5 - 18 GHz (1.7 - 2.4 cm)
- K band: 18 - 26.5 GHz (1.1 - 1.7 cm)
- Ka band: 26.5 - 40 GHz (0.75 - 1.1 cm)

Wavelengths of Infrared

- Infrared: 0.7 to 300 µm wavelength. This region is further divided into the following bands:
- Near Infrared (NIR): 0.7 to 1.5 µm.

• Short Wavelength Infrared (SWIR): 1.5 to 3 µm.
• Mid Wavelength Infrared (MWIR): 3 to 8 µm.
• Long Wanelength Infrared (LWIR): 8 to 15 µm.
• Far Infrared (FIR): longer than 15 µm.
• The NIR and SWIR are also known as the Reflected Infrared, referring to the main infrared component of the solar radiation reflected from the earth's surface. The MWIR and LWIR are the Thermal Infrared.

Wavelengths of visible light
• Red: 610 - 700 nm
• Orange: 590 - 610 nm
• Yellow: 570 - 590 nm
• Green: 500 - 570 nm
• Blue: 450 - 500 nm
• Indigo: 430 - 450 nm
• Violet: 400 - 430 nm

Electromagnetic (EM) Theory
Electric Field (E) E is the effect produced by the existence of an electric charge, e.g. an electron, ion, or proton, in the volume of space or medium that surrounds it. E=F/q F = is the electric force experienced by the particle q= particle charge E= is the electric field where the particle is located Magnetic Field (B) B is the effect produced by a change in velocity of an electric charge q In a major intellectual breakthroughs in the history of physics (in the 1800s), James Clerk Maxwell came up with the four equations which described all EM phenomena and MAXWELL'S EQUATIONS .

Electromagnetic Radiation (EMR)
• The first requirement for remote sensing is to have an energy source to illuminate the target. This energy for remote sensing instruments is in the form of electromagnetic radiation (EMR).
• Remote sensing is concerned with the measurement of EMR returned by Earth surface features that first receive energy from (i) the sun or (ii) an artificial source e.g. a radar transmitter.
• Different objects return different types and amounts of EMR.
• Objective of remote sensing is to detect these differences with the appropriate instruments.
• Differences make it possible to identify and assess a broad range of surface features and their conditions.

AEM energy (radiation) is one of many forms of energy. It can be generated by changes in the energy levels of electrons, acceleration of electrical charges, decay of radioactive substances, and the thermal motion of atoms and molecules.
All natural and synthetic substances above absolute zero (0 Kelvin, -273°C) emit a range of electromagnetic energy.
Most remote sensing systems are passive sensors, i.e. they relying on the sun to generate all the required EM energy.

Polarization (waves)

Polarization (also polarisation) is a property applying to transverse waves that specifies the geometrical orientation of the oscillations. In a transverse wave, the direction of the oscillation is transverse to the direction of motion of the wave, so the oscillations can have different directions perpendicular to the wave direction. A simple example of a polarized transverse wave is vibrations traveling along a taut string (see image); for example, in a musical instrument like a guitar string. Depending on how the string is plucked, the vibrations can be in a vertical direction, horizontal direction, or at any angle perpendicular to the string. In contrast, in longitudinal waves, such as sound waves in a liquid or gas, the displacement of the particles in the oscillation is always in the direction of propagation, so these waves do not exhibit polarization. Transverse waves that exhibit polarization include electromagnetic waves such as light and radio waves, gravitational waves, and transverse sound waves (shear waves) in solids. In some types of transverse waves, the wave displacement is limited to a single direction, so these also do not exhibit polarization; for example, in surface waves in liquids (gravity waves), the wave displacement of the particles is always in a vertical plane.

An electromagnetic wave such as light consists of a coupled oscillating electric field and magnetic field which are always perpendicular; by convention, the "polarization" of electromagnetic waves refers to the direction of the electric field. In linear polarization, the fields oscillate in a single direction. In circular or elliptical polarization, the fields rotate at a constant rate in a plane as the wave travels. The rotation can have two possible directions; if the fields rotate in a right hand sense with respect to the direction of wave travel, it is called right circular polarization, or, if the fields rotate in a left hand sense, it is called left circular polarization.

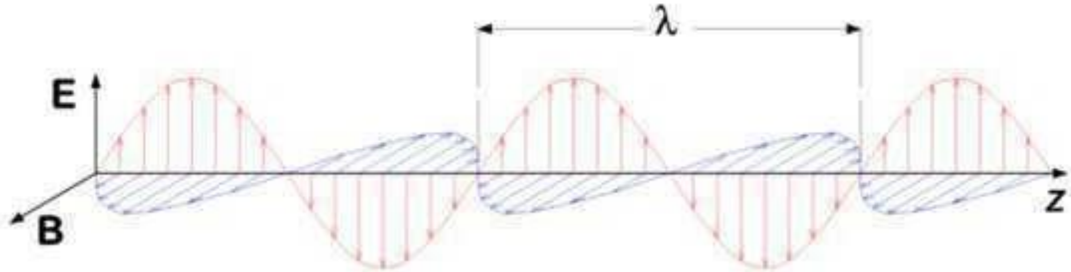
Light or other electromagnetic radiation from many sources, such as the sun, flames, and incandescent lamps, consists of short wave trains with an equal mixture of polarizations; this is called unpolarized light. Polarized light can be produced by passing unpolarized light through a polarizing filter, which allows waves of only one polarization to pass through. The most common optical materials (such as glass) are isotropic and do not affect the polarization of light passing through them; however, some materials—those that exhibit birefringence, dichroism, or optical activity—can change the polarization of light. Some of these are used to make polarizing filters. Light is also partially polarized when it reflects from a surface.

According to quantum mechanics, electromagnetic waves can also be viewed as streams of particles called photons. When viewed in this way, the polarization of an electromagnetic wave is determined by a quantum mechanical property of photons called their spin. A photon has one of two possible spins: it can either spin in a right hand sense or a left hand sense about its direction of travel. Circularly polarized electromagnetic waves are composed of photons with only one type of spin, either right- or left-hand. Linearly polarized waves consist of equal numbers of right and left hand spinning photons, with their phase synchronized so they superpose to give oscillation in a plane.

Polarization is an important parameter in areas of science dealing with transverse waves, such as optics, seismology, radio, and microwaves. Especially impacted are technologies such as lasers, wireless and optical fiber telecommunications, and radar.
Refers to orientation of the electric field E If both E and B remain in their respective planes, the radiation is called "plane or linearly polarised" :

- vertically polarized (E is parallel to the plane of incidence)
- horizontally polarized (E is perpendicular to the plane of incidence) Plane of incidence = the plane defined by the vertical and the direction of propagation.

If instead of being confined to fixed direction, E rotates in the xy plane with constant amplitude, it is said to be circularly polarised (either right- or left-hand circular (clockwise/anti-clockwise respectively) Circularly polarised light consists of two perpendicular EM plane waves of equal amplitude and 90° difference in phase. The light illustrated is right-hand circularly polarized



A "vertically polarized" electromagnetic wave of wavelength λ has its electric field vector **E** (red) oscillating in the vertical direction. The magnetic field **B** (or **H**) is always at right angles to it (blue), and both are perpendicular to the direction of propagation (**z**).

Fig. 4.7

Wavefronts and Rays

Imagine you throw a rock into a pond. Seen from the side, at the level of the water, the ripples look like this:

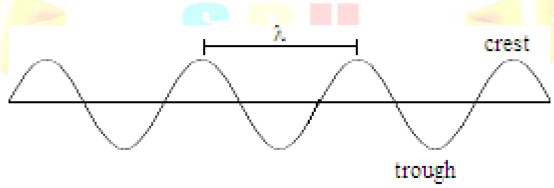


Fig. 4.8

The distance between one ripple and the next is called the wavelength, λ. The high points are called crests, and the low points are the troughs.
If instead you look down on the pond, as if from a hovering helicopter, the ripples are round, and spreading outwards (diverging). The technical term for ripples is wavefronts. The arrows are pointing in the direction the waves are moving, and they are called rays. Notice that the rays are always perpendicular to the wavefronts. In other words, the wavefront always moves in a direction at right angles to itself.

As the waves move farther and farther from the center, where the rock hit the water, the wavefronts are larger and larger circles. But if you look at a small piece of the wavefront, it nearly looks flat.

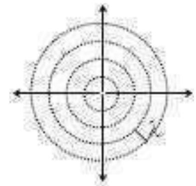


Fig 4.9

For an electromagnetic wave, the wavefront is represented as a surface of identical phase, and can be modified with conventional optics. For instance, a lens can change the shape of optical wavefronts from planar to spherical as the lens introduces a spatial phase variation across the beam shape.

Wave Model of Electromagnetic Radiation

Maxwell theory tells us that EMR is an EM wave that travels through space at the speed of light, c, which is 3 x 108 meters per second (hereafter referred to as ms^{-1}) or 186,282.03 miles s-1 (1 foot per nanosecond). The EM wave consists of two fluctuating fields—one electric and the other magnetic. The two vectors are at right angles (orthogonal) to one another, and both are perpendicular to the direction of travel.

EMR is generated when an electrical charge is accelerated.

The wavelength of EMR (λ) depends upon the length of time that the charged particle is accelerated and its frequency (ν) depends on the number of accelerations per second.

Wavelength is the mean distance between maxima (or minima) of a roughly periodic pattern and is normally measured in micrometers (mm) or nanometers (nm).

Frequency is the number of wavelengths that pass a point per unit time. A wave that sends one crest by every second (completing one cycle) is said to have a frequency of one cycle per second or one hertz, abbreviated 1 Hz.

Inverse-square law

In physics, an inverse-square law is any physical law stating that a specified physical quantity or intensity is inversely proportional to the square of the distance from the source of that physical quantity. The fundamental cause for this can be understood as geometric dilution corresponding to point-source radiation into three-dimensional space (see diagram). Mathematically formulated:

The divergence of a vector field which is the resultant of radial inverse-square law fields with respect to one or more sources is everywhere proportional to the strength of the local sources, and hence zero outside sources. Newton's law of universal gravitation follows an inverse-square law, as do the effects of electric, magnetic, light, sound, and radiation phenomena.

Radar energy expands during both the signal transmission and also on the reflected return, so the inverse square for both paths means that the radar will receive energy according to the inverse fourth power of the range.

In order to prevent dilution of energy while propagating a signal, certain methods can be used such as a waveguide, which acts like a canal does for water, or how a gun barrel restricts hot gas expansion to one dimension in order to prevent loss of energy transfer to a bullet.

Wave Attenuation and Absorption

In physics / engineering, the gradual reduction in the intensity of a signal (beam of waves) which is propagating through a material is known as the attenuation. It is a common phenomenon experienced by any kind of wave or signal propagating through a medium. For example, acoustic waves are attenuated by water, X- rays are attenuated by lead, and seismic waves are attenuated as they propagate through the Earth. Normally, attenuation is an exponential function of the path length through the medium. In other words, the extent of the attenuation of a wave through a given medium depends on the path length. In addition, the attenuation of a wave or beam depends on the frequency of the wave and the medium through which the wave propagates. The units of measuring attenuation are dB/m, dB/cm or dB/km (decibels per unit path length).

The extent of the attenuation of electromagnetic waves depends on the medium through which the waves propagate. For instance, the extent of attenuation of a given EM wave through water and a plasma is very different. The attenuation of EM waves occurs due to both absorption and scattering of photons. The absorption of EM waves in a matter is a result of several types of interactions (photoelectric effect, Compton effect, pair production) take place between EM waves and matter.

Attenuation is a very important factor in telecommunication as the attenuation limits the effective range of signals. In fiber optics, the attenuation of signals through the medium is commonly known as the transmission loss. Fiber optic technology is widely being used for long-range communication as the attenuation in optical fibers is notably low compared to other communication technologies.

Attenuation of ultrasound waves in a given medium is the reduction in amplitude of the waves traveling through the medium and, depends on the medium, the path length and the frequency of the waves. The extent of the attenuation determines the quality of images. Therefore, attenuation of ultrasound waves is a very important factor in ultrasound imaging.

The term Absorption is used in different fields of study with different meanings. In electromagnetism, the absorption of energy of EM waves by a material is commonly referred to as the absorption. In this process, the absorbed energy appears as the heat of the medium or another form of energy such as the vibrational and rotational energy of the atoms or molecules of the medium. The absorption of EM waves depends on several factors such as the frequency of EM waves, the medium, path length, and concentration of the absorbing medium. Light waves can propagate through a perfectly transparent material without any reduction in the amplitude. In practice, transparent glasses permit the light waves to pass through them with a

relatively low reduction in the amplitude. However, light waves passing through highly opaque mediums lose their total amount of energy and eventually disappear.
In acoustic physics, the absorption of sound waves by a material medium is commonly referred to as absorption. Absorption of sound waves is a popular area of study, especially in sound proofing. Normally, soft, flexible, porous materials are good sound absorbers whereas hard, heavy materials reflect sound waves. The absorbed sound energy is mainly converted into heat of the absorbing medium.

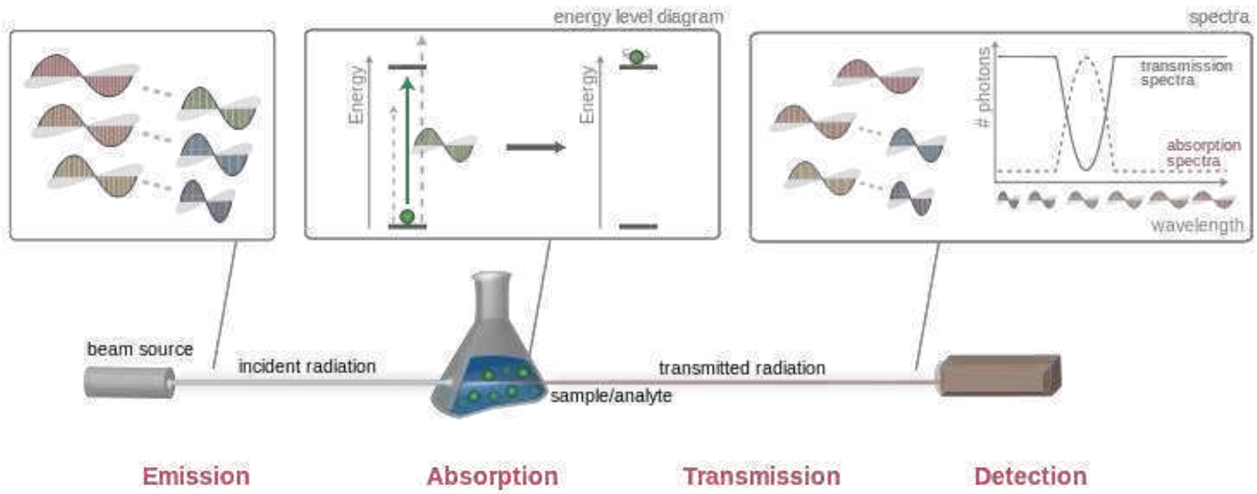


Fig. 4.10

Radio propagation is the behavior of radio waves when they are transmitted, or propagated from one point on the Earth to another, or into various parts of the atmosphere. As a form of electromagnetic radiation, like light waves, radio waves are affected by the phenomena of reflection, refraction, diffraction, absorption, polarization and scattering. Radio and Optical waves have the same nature with a difference in wavelengths. Both are electromagnetic waves obeying reflection, refraction, and diffraction. If these characteristics were not there, the existing radio and optical systems would not have worked. For instance, for radio waves reflection is used in sky wave transmission. For optical waves, reflection is used for propagation of light waves in optical fibers. For other characteristics, there are many examples. Of course, in some cases these characteristics would trouble the radio and optical transmissions, either.

Terrestrial Propagation of Long Electromagnetic Waves deals with the propagation of long electromagnetic waves confined principally to the shell between the earth and the ionosphere, known as the terrestrial waveguide. Wave propagation is characterized almost exclusively by mode theory.

A **Communications satellite** is an artificial satellite that relays and amplifies radio telecommunications signals via a transponder; it creates a communication channel between a source transmitter and a receiver at different locations on Earth. Communications satellites are used for television, telephone, radio, internet, and military applications. There are over 2,000 communications satellites in Earth's orbit, used by both private and government organizations.

Wireless communication uses electromagnetic waves to carry signals. These waves require line-of-sight, and are thus obstructed by the curvature of the Earth. The purpose of communications satellites is to relay the signal around the curve of the Earth allowing communication between widely separated points. Communications satellites use a wide range of radio and microwave frequencies. To avoid signal interference, international organizations have regulations for which frequency ranges or "bands" certain organizations are allowed to use. This allocation of bands minimizes the risk of signal interference.

Communications satellites usually have one of three primary types of orbit, while other orbital classifications are used to further specify orbital details.

- Geostationary satellites have a geostationary orbit (GEO), which is 35,786 kilometres (22,236 mi) from Earth's surface. This orbit has the special characteristic that the apparent position of the satellite in the sky when viewed by a ground observer does not change, the satellite appears to "stand still" in the sky. This is because the satellite's orbital period is the same as the rotation rate of the Earth. The advantage of this orbit is that ground antennas do not have to track the satellite across the sky, they can be fixed to point at the location in the sky the satellite appears.
- Medium Earth orbit (MEO) satellites are closer to Earth. Orbital altitudes range from 2,000 to 35,786 kilometres (1,243 to 22,236 mi) above Earth.
- The region below medium orbits is referred to as low Earth orbit (LEO), and is about 160 to 2,000 kilometres (99 to 1,243 mi) above Earth.

As satellites in MEO and LEO orbit the Earth faster, they do not remain visible in the sky to a fixed point on Earth continually like a geostationary satellite, but appear to a ground observer to cross the sky and "set" when they go behind the Earth. Therefore, to provide continuous communications capability with these lower orbits requires a larger number of satellites, so one will always be in the sky for transmission of communication signals. However, due to their relatively small distance to the Earth their signals are stronger

The Telephone Network

The telephone network began in the late 1800s which was referred to as plain old telephone system (POTS). It was orignally analog, but with the advancement in computer technology the network started to carry data as well as voice in 1980's. It is now both digital and analog.

Major Components

The telephone network is made of three major components - the local loops, the trunks and the switching office.
The local loop connects the subscriber to the nearest end office (or local central office) through a twisted-pair cable. It has a bandwidth of 4000Hz. The trunk is a transmission media that connects switching offices. It handles a lot of connections through multiplexing. these are usually optical fibers or satellite links.
The switching office establishes a connection between two subscribers. The connection between two subscribers is not permanent and will only be made upon request. Connections

are limited by the total bandwidth of a transmission media therefore having permanent idle lines would limit the services of the network.

LATA

The local telephone network is referred to as Local Access Transport Areas (LATA). LATAs are made up of multiple local loops connected to a tandem office. Services of Comon Carriers (telephone companies) within a LATA are called intra-LATA services. These carriers are refered to as Local Exchange Carriers (LEC). LEC has to types. The Incumbent Local Exchange Carriers (ILEC) is the original company that set up the LATA. To avoid cost for new cabling, Competitive Local Exchange Carriers (CLEC) were allowed to use the LATA of the ILEC for their own services. Services between LATAs (Inter-LATA services) are handled by Interexchange Carriers (IXC), commonly referred to as long-distance companies. LECs are also allowed to become IXCs. To allow multiple IXCs to use a LATA, a Point of Presence (POP) switching office is created for each IXC.A caller, who needs to connect to a receiver in another LATA, first connects to an end switch then, either directly or through a tandem office, to a POP of the caller's choice. The call then goes from the POP in the caller's LATA to the POP of the same IXC in the reciever's LATA then down to the switching offices and finally to the telephone of the receiver.

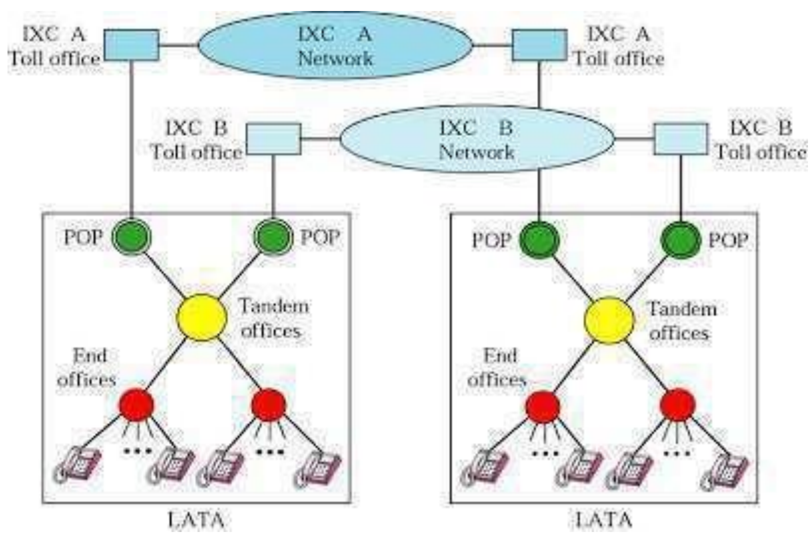


Fig. 4.11

DSL Technologies

A Digital Subscriber Line makes use of the current copper infrastructure to supply broadband services. A DSL requires two modems, one at the phone companies end and one at the subscribers end. The use of the term modem is not entirely correct because technically a DSL modem does not do modualtion/demodulation as in a modem that uses the normal telephone network. DSL's also have the added benefit of transmitting telephone services on the same set of wire as data services. DSL's common in many flavor, and are sometimes referred to as xDSL, the x standing for the specific type.

It has been believed that the upper limit for transmitting data on analog phone lines was 56 kb/s. This limit is set using the maximum possible bandwidth and no compression. The reason for this limit is that POTS or Plain Old Telephone Service uses the lower 4 Khz only. The limit imposed by the POTS lines does not take advantage of all the bandwidth available on copper, which is on the order of 1 Mhz. The xDSL technologies take advantage of this difference and uses the upper frequencies for data services. Previously this was not possible because of the interference that the data services would cause in the POTS band. Advances in digital signal processing have eliminated the near-end crosstalk that results from the use of the upper bandwidth for data. The new DSP technologies allow data and POTS to be transmitted on the same set of copper wires without interfering with each other. DSL technologies were initially tested for use with video on demand (VOD) and interactive television (ITV) services. Lack of a "killer application" for these services and competition from the cable TV industry in these areas forced the telephone companies to look for a different application for their technologies. With the popularity of the World Wide Web and telecommuting on the rise the DSL technologies moved to providing network and phone services to the home. Other areas where DSL technologies are targeted for are Intranet access, LAN to LAN connections, Frame Relay, ATM Network access, and leased line provisioning.

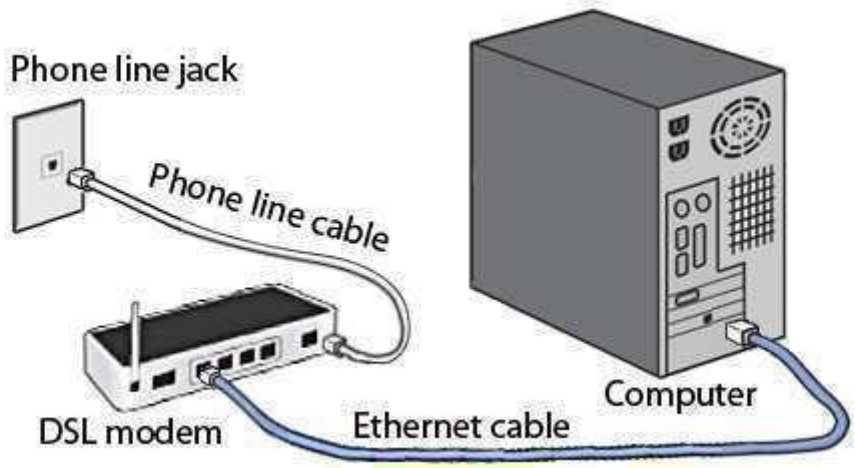


Fig. 4.12

ADSL-Asymmetric Digital Subscriber Line

The most promising of the DSL technologies is ADSL or Asymmetric Digital Subscriber Line. ADSL looks to make the most impact in residential access and the SOHO (Small Office Home Office) market. Just like the name implies ADSL is asymmetric, meaning that the downstream bandwidth is higher than the upstream bandwidth. Downstream refers to traffic in the direction towards the subscriber, and upstream refers to data sent from the subscriber back to the network. This is done because of the kinds traffic that ADSL is designed to carry. Asymmetry is used to increase the downstream bandwidth. This works because all of the downstream signals can be of the same amplitude thus eliminating crosstalk between downstream channels. Upstream signals would have to put up with more interference because the amplitude of the upstream signals would be of smaller amplitude because the are originating from different distances. The asymmetric nature of ADSL lends itself well to applications like the web and client server applications.

To achieve the asymmetry ADSL divides its bandwidth into four classes of transport.

1. higher bandwidth simplex channel
2. lower bandwidth duplex channel
3. duplex control channel
4. POTS channel

Transmission on the high bandwidth simplex channel and the lower bandwidth duplex channel do not interfere in any way with the POTS channel. So ADSL can carry both data a POTS on the same medium, which makes it ideal for residential and small office use.

ADSL bandwidth is currently standardized by ANSI (American National Standards Institute). Tables 1 and 2 detail the four transport classes which are based on multiples of T-1 (1.5 Mb/s) downstream bandwidth. There are also three more classes that are based on the European E-1 (2.0 Mb/s) standard which is shown in the second chart. These classes are all based on the maximum bandwidth available on each channel. The actual rates depend on factors such as wire gauge,local loop length, and line condition. In this case, the local loop length is the

Fig. 4.13

HDSL- High-data-rate Digital Subscriber Line

The most common DSL deployed today is HDSL. HDSL is mostly used to provision other services by telephone companies. HDSL symmetrically delivers 1.544 Mb/s over two sets of copper twisted pair. Which is the same rate as a T-1 type connection. This allows telco's (short for telephone companies) to use HDSL to deliver T-1 services. HDSL's operating range is about 12,000 feet, and it is possible to extend that by using repeaters along the line to the customer. HDSL is mostly used to deploy PBX network connections , interexchange POP's (Point Of Presence), and directly connecting servers to the Internet.

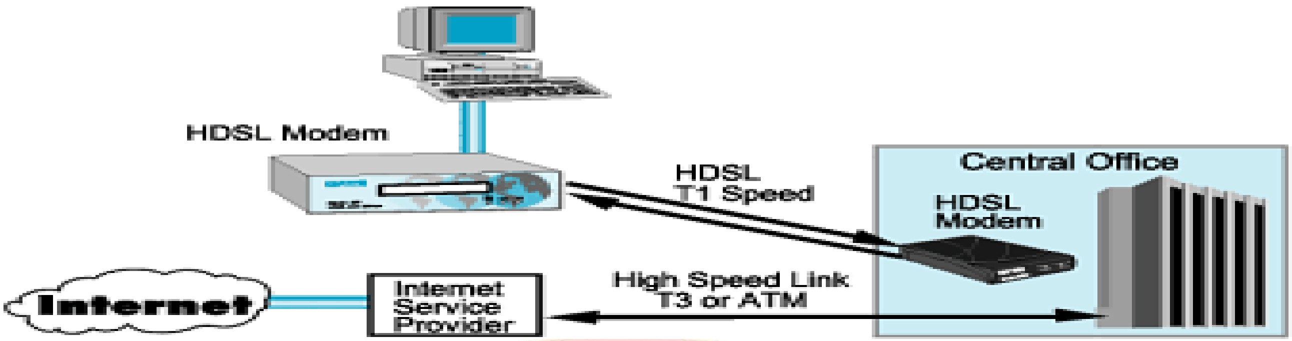


Fig. 4.14

SDSL -Single-line Digital Subscriber Line also know as Symmetric Digital Subscriber Line

Similar to HDSL, SDSL delivers the same 1.544 Mb/s, but it does it on a single set of twisted pair of copper. This limits SDSL's reach to 10,000 feet. SDSL could take hold in niche markets like residential video conferencing or connecting LAN's over short distances.

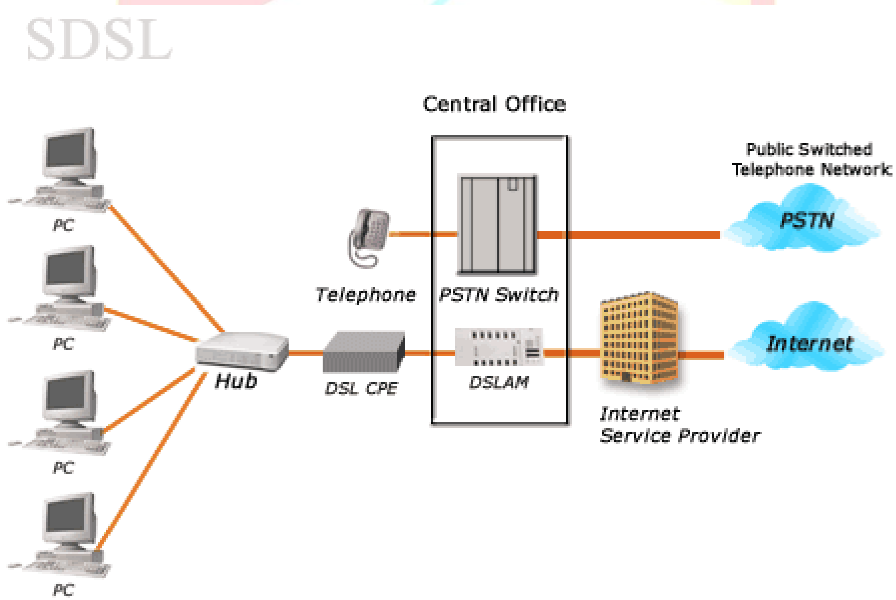


Fig. 4.15

VDSL- Very-high-rate Digital Subscriber Line

VDSL technology operates on a single set of copper twisted pair, and delivers data in the range of 13 Mb/s to 52 Mb/s. This high bandwidth does not come without a price, the range of VDSL is limited to between 1,000 and 4,500 feet. The VDSL standard is still in the works but there are already applications for the technology. One use for it is in getting high data rate services from the telephone companies central office to the subscriber via a FTTN (Fiber To The Neighborhood) network. FTTN encompasses the Fiber To The Curb technologies and uses VDSL as the customers connection to the telephone companies fiber based network.

VDSL would be used to connect premises distribution networks to the Optical Network Unit or ONU. The optical network unit is in turn connected via fiber optical line to the telco's central office.

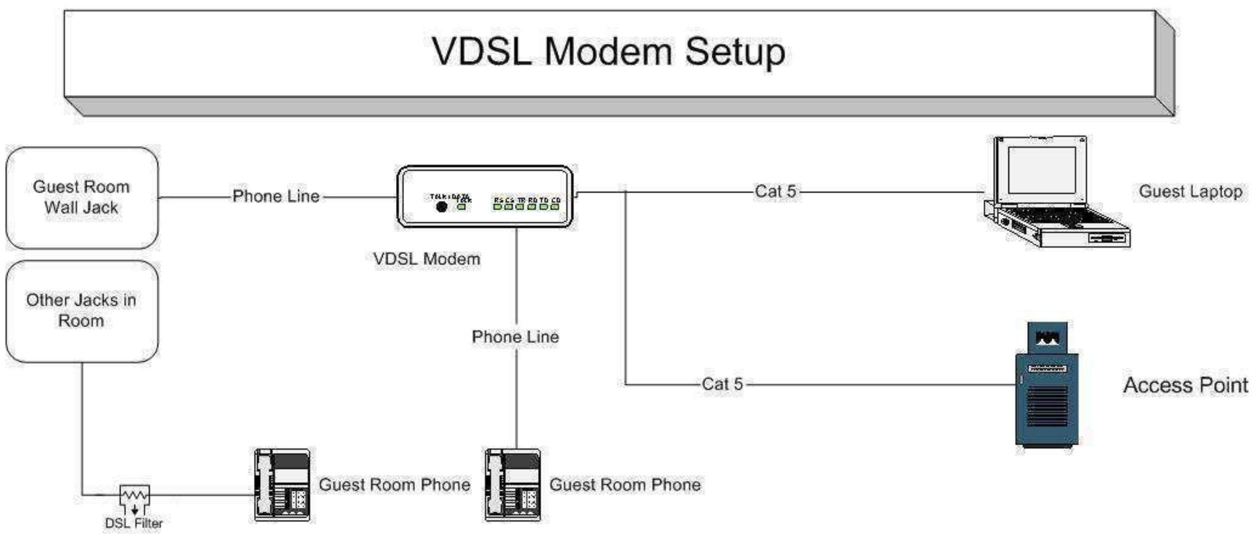


Fig. 4.16

Cable TV network for data transfer

Cable network is a system receiving and distributing RF signals mainly inside apartment buildings. The borderline between a community antenna system and a cable TV network can be defined in many different ways, e.g. in Poland a cable network is defined as RF installation located in more than one building and having more than 250 outlets.
Cable TV was primarily planned to be signal installation allowing distribution of large (above 60) number of programs to large or very large group of subscribers. In the beginning there were used the same channels as for terrestrial television only.

Data transmission to the subscriber.

There are usually used only 60 channels for television transmission. On the assumption that, for the reason of possible distortions, there are left free the channels of terrestrial transmitters (usually 8) and 4 channels for modulators (of e.g. VCRs), it is still 22 channels available for data transmission. In practice, the number is further decreased because some channels have to be skipped due to distortions caused by other transmitters etc., so the real number is around 10.

These channels can be used for digital data broadcasting to subscribers (forward direction). Due to high quality of cable transmission (high S/N ratio, even including some specific distortions in cable networks), especially in the direction to subscribers, it is possible to use complex multi-level modulations. Such modulations ensure fast transmission within low bandwidth, i.e. high efficiency.

Typical examples are the 16QAM and 64QAM modulations. In practice, they are only used for broadcast channels, because they require relatively high signal to noise ratio. The advantage of this kind of modulation is high channel capacity, equal 4 b/Hz/s for 16QAM, and 6 b/Hz/s for 64QAM.

Reverse transmission - the return channel.

Obviously the users must have possibility of reverse transmission to the head station. Because of use of distribution amplifiers, the only possibility is frequency division, i.e. the forward transmission is performed in the range of television channels and the reverse transmission - in 5-65 MHz range. On account of the specificity of this kind of transmission, it is required to use interference-resistant modulations.

For this purpose there are usually used BPSK and QPSK modulations. Their basic advantages are high resistance to distortions and simplicity of the modulators and demodulators. These are the simplest phase modulations, with binary phase-shift keying and quadrature phase-shift keying adequately. The channel capacity is equal 1 b/Hz/s for BPSK and 2 b/Hz/s for QPSK.

Band selection for the return channel.

We have mentioned before that for the reverse transmission in cable networks there have been chosen frequencies lying below forward band, i.e. the 5-65 MHz range. It's worth trying to understand why.

There were two possible variants, either using the band lying below the lowest TV channel, or above the highest one. The frequencies above 862 MHz are less vulnerable to external interferences, as the range is a subject to regulations and the transmitters have limited output power.

However, distribution of so high frequency signals in cable TV networks encounters various problems, related to increase of cable attenuation and decrease of shielding effectiveness. In addition, the higher frequency, the bigger trouble with making filters with steep edges of frequency characteristics.

By contrast, the band below 65 MHz is the most commonly used frequency band, thus the environment is full of interferences. It is interfered by CB transceivers, household devices, car ignition systems, lighting controllers, computers etc. However, the basic advantage of this band for cable applications is low attenuation of the cables and possibility of making efficient filters. Besides that, it is easier to build active devices working in lower frequency bands.

In the very beginning, the upper frequency of the return channel was 30 MHz, to avoid any possibility of interference with the lowest TV channel beginning at 47 MHz. Later, since the lower channels were not used any more, the band has been widened.

Throughput of the return channel.

Now we will try to estimate the throughput of the return channel. Transmission speed depends on the available bandwidth and spectral efficiency of the modulation used.

Rb=B*n
Where:
Rb - transmission speed in bps (bits per second)
B - bandwidth in Hz
n - spectral efficiency in bps/Hz, showing the number of bits that can be coded by one change of the carrier; n describes capacity of the modulation used (it is limited by the ratio of total signal power over the bandwidth and total noise power over the bandwidth).
Transmission speed is proportional to available bandwidth and channel capacity.
The more complex modulation, the higher n, reaching even 10 for 1024QAM modulation.

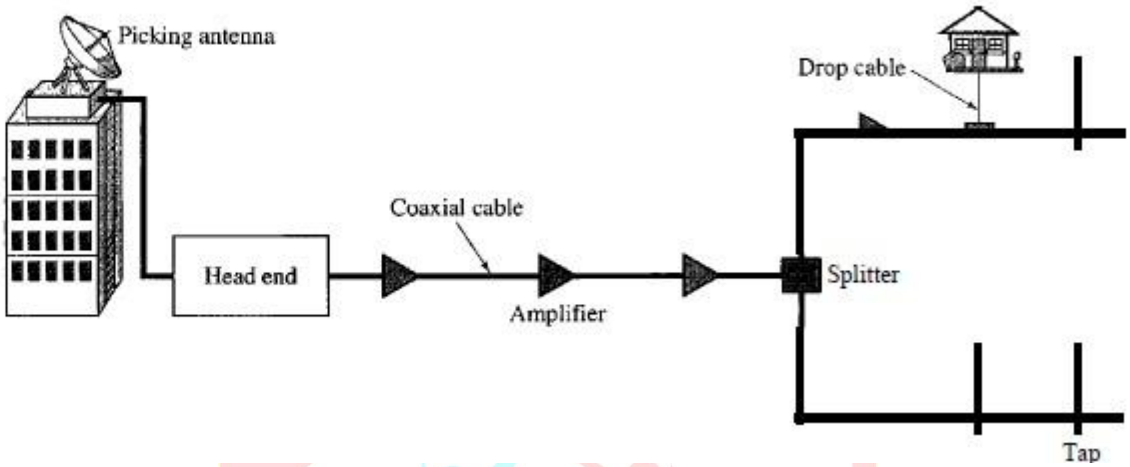


Fig. 4.17

Cable companies are now competing with telephone companies for the residential customer who wants high-speed data transfer. DSL technology provides high-data-rate connections for residential subscribers over the local loop. However, DSL uses the existing unshielded twisted-pair cable, which is very susceptible to interference. This imposes an upper limit on the data rate. Another solution is the use of the cable TV network. In this section, we briefly discuss this technology.

Bandwidth

Even in an HFC system, the last part of the network, from the fiber node to the subscriber premises, is still a coaxial cable. This coaxial cable has a bandwidth that ranges from 5 to 750 MHz (approximately). To provide Internet access, the cable company has divided this bandwidth into three bands: video, downstream data, and upstream data, as shown

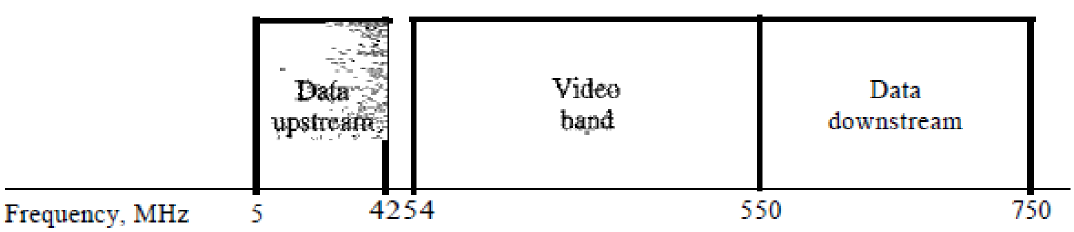


Fig. 4.18

Downstream Video Band

The downstream video band occupies frequencies from 54 to 550 MHz. Since each TV channel occupies 6 MHz, this can accommodate more than 80 channels.
Downstream Data Band
The downstream data (from the Internet to the subscriber premises) occupies the upper band, from 550 to 750 MHz. This band is also divided into 6-MHz channels. Modulation Downstream data band uses the 64-QAM (or possibly 256-QAM) modulation technique.

UNIT-V

In Communication Networks External electromagnetic signals can cause incorrect delivery of data. By this, data in the communication Networks can be received incorrectly, data can be lost or unwanted Communication Networks data can be generated. Any of these problems are called transmission errors in communication networks.

Transmission errors are caused by:

1) thermal noise {Shannon}
2) impulse noise (e..g, arcing relays)
3) signal distortion during transmission (attenuation)
4) crosstalk
5) voice amplitude signal compression
6) quantization noise (PCM)
7) jitter (variations in signal timings)
8) receiver and transmitter out of synch

The local loops are still analog twisted copper pairs and will continue to be so for years due to the enormous expense of replacing them. While errors are rare on the digital part, they are still common on the local loops. Furthermore, wireless communication is becoming more common, and the error rates here are orders of magnitude worse than on the interoffice fiber trunks. The conclusion is: transmission errors are going to be with us for many years to come. We have to learn how to deal with them.

As a result of the physical processes that generate them, errors on some media (e.g., radio) tend to come in bursts rather than singly. Having the errors come in bursts has both advantages and disadvantages over isolated single-bit errors. On the advantage side, computer data are always sent in blocks of bits. Suppose that the block size is 1000 bits and the error rate is 0.001 per bit. If errors were independent, most blocks would contain an error. If the errors came in bursts of 100 however, only one or two blocks in 100 would be affected, on average. The disadvantage of burst errors is that they are much harder to correct than are isolated errors.

When data is being transmitted from one machine to another, it may be possible that data become corrupted on its, way. Some of the bits may be altered, damaged or lost during transmission. Such a condition is known as error.

The error may occur because of noise on line, attenuation and delay distortion. For reliable communication, it is important that errors are detected and corrected.

Errors are introduced in the data bits during their transmission across a data network. These errors can be categorized as:

1. **Content Error: Error contained in a received frame are termed content error.**
2. **Flow integrity error:Flow integrity errors refer to the lost or duplicate data frames and acknowledgements.**

Data link error control takes both types of errors.

Content errors are detected using parity check or cyclic redundancy check bits. The check bits are added as the trailer in a frame at the sending end.

Type of Errors

There are two main types of errors in transmissions:

1. Single bit error
2. Burst error

Single bit error: It means only one bit of data unit is changed from 1 to 0 or from 0 to 1 as shown in fig.

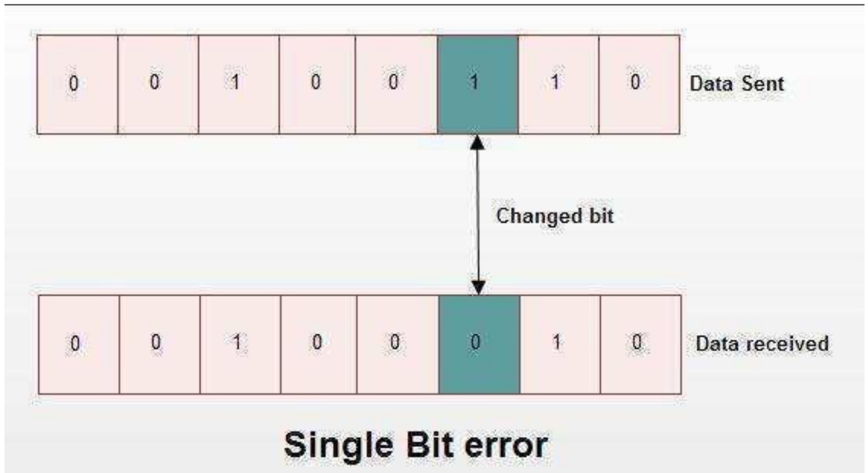


Fig. 5.1

Single bit error can happen in parallel transmission where all the data bits are transmitted using separate wires. Single bit errors are the least likely type of error in serial transmission.

Burst Error: It means two or more bits in data unit are changed from 1 to 0 from 0 to 1 as shown in fig.

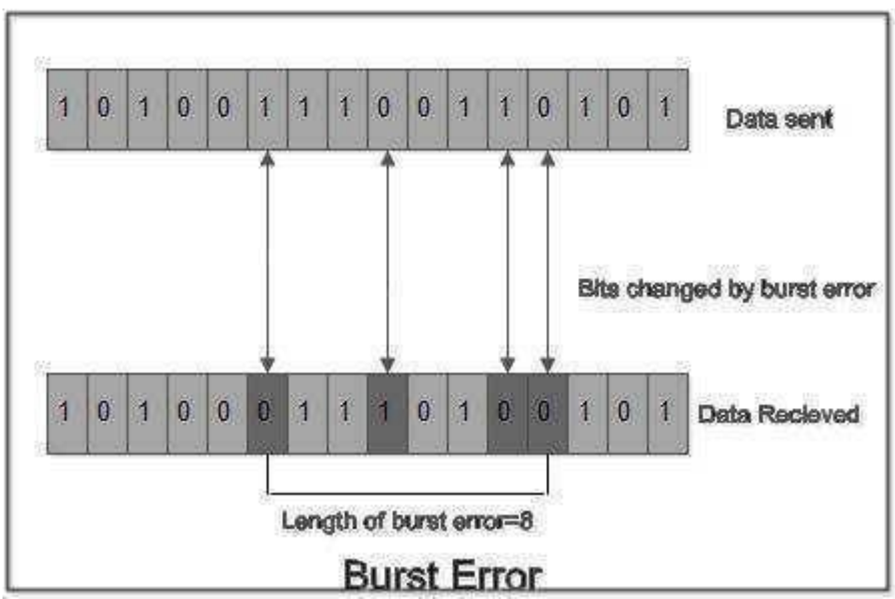


Fig. 5.2

In burst error, it is not necessary that only consecutive bits are changed. The length of burst error is measured from first changed bit to last changed bit. As shown in fig. length of burst error is 8, although some bits are unchanged in between. Burst error is most likely to occur in a serial transmission. The noise occurring for a longer duration affects multiple bits. The number of bits affected depends on the data rate & duration of noise. For e.g. if data rate is 1 kbps, a noise of 1/100 second can affect 10 bits.

There are several caused of content error:-

1. Signal impairment
2. Loss of synchronization.
3. Scramblers
4. Tranmsission channel switching

Error Detection and Correction

Error Detection

Error detection is the process of detecting the error during the transmission between the sender and the receiver.

Types of error detection

- Parity checking
- Cyclic Redundancy Check (CRC)
- Checksum

error detection :adding enough "extra" bits to deduce that there is an error but not enough bits to correct the error. If only error detection is employed in a network transmission retransmission is necessary to recover the frame (data link layer) or the packet (network layer). At the data link layer, this is referred to as ARQ (Automatic Repeat reQuest).

error correction : requires enough additional (redundant) bits to deduce what the correct bits must have been. Examples Hamming Codes FEC = Forward Error Correction found in MPEG-4 for streaming multimedia.

Codeword: a legal dataword consisting of m data bits and r redundant bits.
Error detection involves determining if the received message matches one of the legal codewords.

Hamming distance: the number of bit positions in which two bit patterns differ. Starting with a complete list of legal codewords, we need to find the two codewords whose Hamming distance is the smallest. This determines the Hamming distance of the code.

Error Correcting Codes

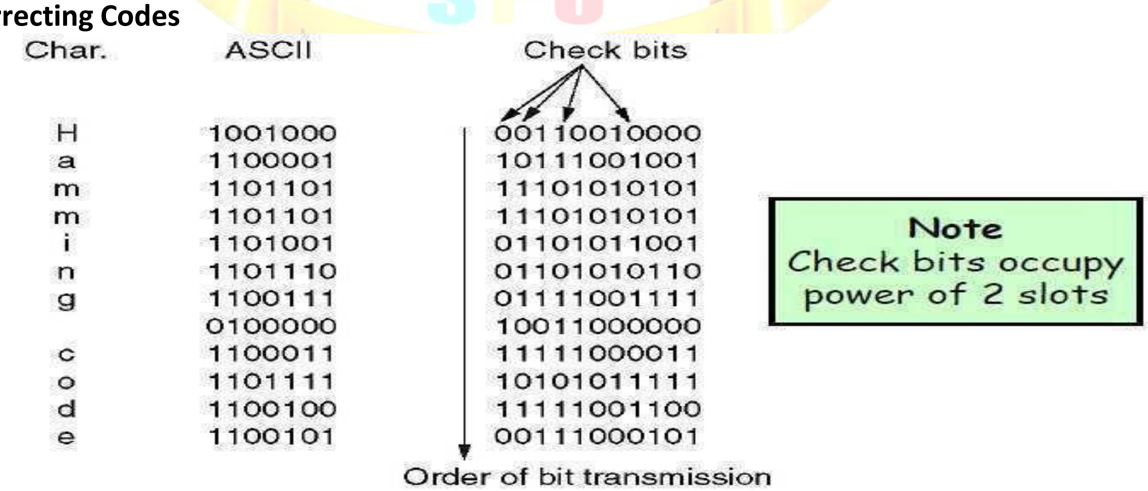


Fig. 5.3

(a) A code with poor distance properties (b) A code with good distance properties

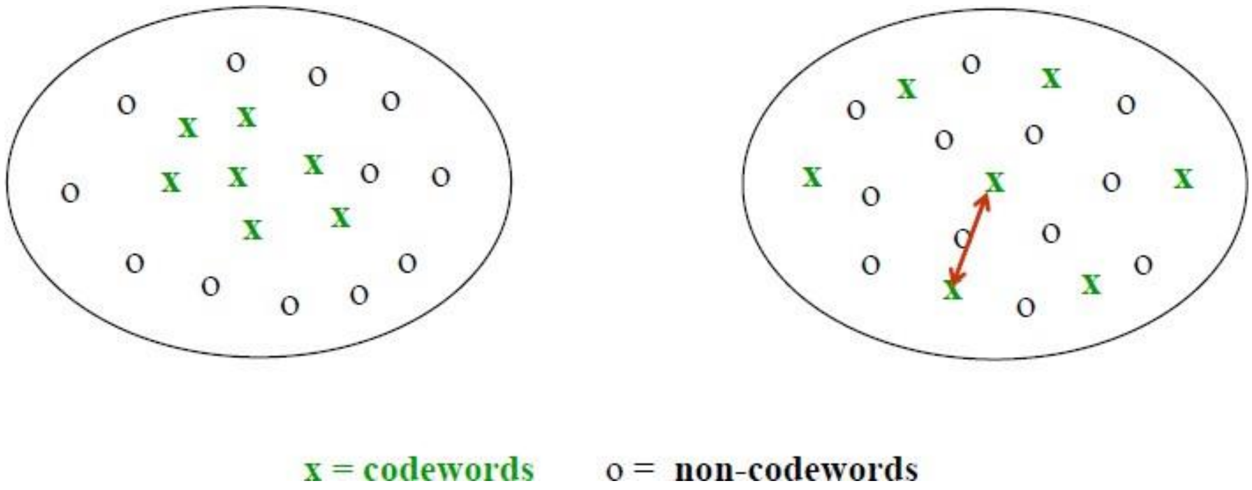


Fig. 5.4

Hamming Codes Hamming Codes

• T o detect d single bit errors, you need a d+1 code distance.

• T o correct d single bit errors, you need a 2d+1 code distance.

In general, the price for redundant bits is too expensive to do error correction for network messages.

Network protocols use error detection and ARQ.

Error Detection Error Detection Remember – errors in network transmissions are bursty.

The percentage of damage due to errors is lower. It is harder to detect and correct network errors.

• Linear codes – Single parity check code : take k information bits and appends a single check bit to form a codeword. – Two-dimensional parity checks

• I P Checksum

• Polynomial Codes Example: C‘C (Cyclic ‘edundancy Checking)

General Error Detection System

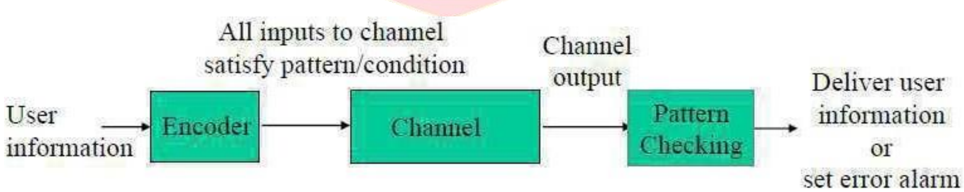


Fig. 5.5

Error Detection System Using Check Bits

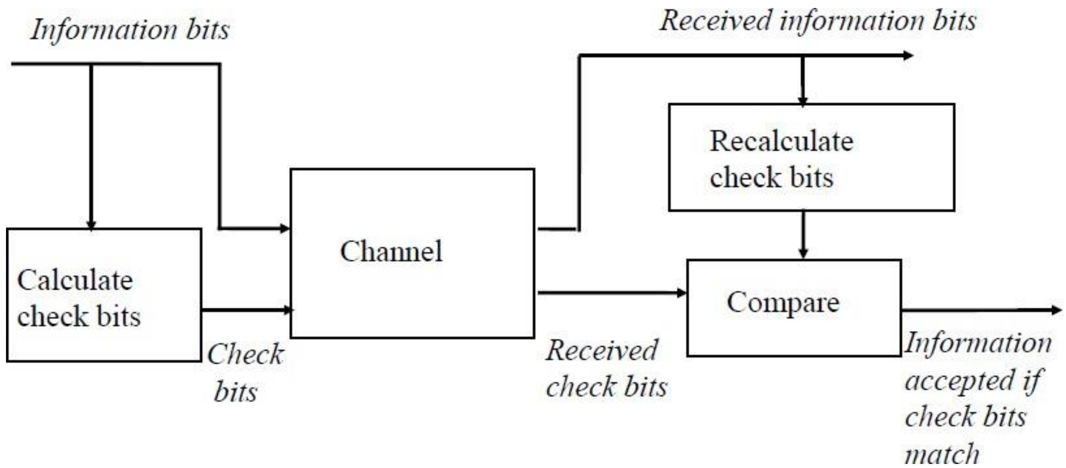


Fig. 5.6

Two-dimensional dimensional Parity Check C1ode

$$\begin{array}{ccccc|c} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 & 0 \\ \hline 1 & 0 & 0 & 1 & 1 & 1 \end{array}$$

Last column consists of check bits for each row

Bottom row consists of check bit for each column

Fig. 5.7

$$\begin{array}{ccccc|c} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 & 0 \\ \hline 1 & 0 & 0 & 1 & 1 & 1 \end{array}$$

One error

$$\begin{array}{ccccc|c} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 \\ \hline 1 & 0 & 0 & 1 & 1 & 1 \end{array}$$

Two errors

$$\begin{array}{ccccc|c} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 \\ \hline 1 & 0 & 0 & 1 & 1 & 1 \end{array}$$

Three errors

$$\begin{array}{ccccc|c} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 \\ \hline 1 & 0 & 0 & 1 & 1 & 1 \end{array}$$

Four errors

Arrows indicate failed check bits

Fi

Preapred and Compiled by: Sunil Kushwaha

Fig. 5.8

Internet Checksum

Used extensively.

- Implemented using shift-register circuits for speed advantages.
- Also called C'C (cyclic redundancy checking) because these codes generate check bits.
- Polynomial codes :: bit strings are treated as representations of polynomials with ONLY binary coefficients (0's and 1's).

T h e k bits of a message are regarded as the coefficient list for an information polynomial of degree k-1

$$I :: i(x) = i_{k-1} x^{k-1} + i_{k-2} x^{k-2} + \dots + i_1 x + i_0$$

Example: 1 0 1 1 0 0 0

$$i(x) = x^6 + x^4 + x^3$$

Fig. 5.9

Encoding process takes i(x) produces a codeword polynomial b(x) that contains information bits and additional check bits that satisfy a pattern.

- Let the codeword have n bits with k information bits and n-k check bits.
- We need a generator polynomial of degree n-k of the form

$$G = g(x) = x^{n-k} + g_{n-k-1} x^{n-k-1} + \dots + g_1 x + 1$$

Fig. 5.10

CRC Codeword CRC Codeword

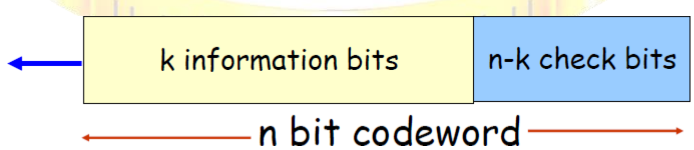


Fig. 5.11

Polynomial Arithmetic

Addition: $(x^7 + x^6 + 1) + (x^6 + x^5) = x^7 + (1+1)x^6 + x^5 + 1$
$= x^7 + x^5 + 1$

Multiplication: $(x+1)(x^2 + x + 1) = x^3 + x^2 + x + x^2 + x + 1 = x^3 + 1$

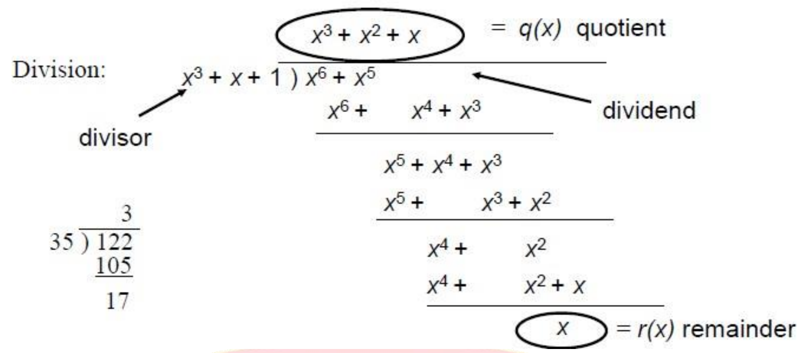


Fig. 5.12

CRC Algorithm
CRC Steps:

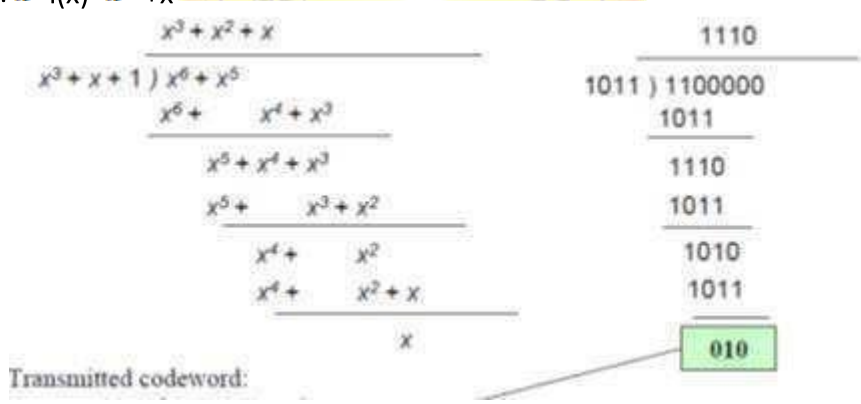
(i) Multiply i(x) by x^{n-k} (puts zeros in (n-k) low order positions).
(ii) Divide x^{n-k} i(x) by g(x)

Quotient remainder

$x^{n-k} j(x)=g(x)q(x)+r(x)$

(iii) Add remainder r(x)to xn-k i(x)
(puts check bits in the n-k low order positions):
b(x) = x^{n-k} *i(x)+r(x) ------------- transmitted codeword*

Information: (1,1,0,0) $\longrightarrow$ $i(x)=x^3+x^2$
Generator Polynomial: g(x)= x^3+x+1
Encoding: x^3i(x)=x^6 +x^5



b(x)=x^6+ x^5+x----------- b=(1,1,0,0,0,1,0)

Fig.

Cyclic Redundancy Checking

Calculation of the polynomial code of the polynomial code checksum checksum.

Generator Polynomial Properties Generator Polynomial Properties for Detecting Errors

Single bit errors: $e(x)=x^i$ $0\leq I \leq n-1$

If g(x) has more than one term, it cannot divide e(x).

Double bit errors: $e(x)= x^i$ i + x^j $0 \leq I \leq j \leq n-1$

$=x^4 (1+x^{j-I})$

If g(x) is primitive, it will not divide $(1+x^{j-I})$ *for* $j-1\leq 2^{n-k}-1$

Odd number of bit errors: e(1) =1 If number of error is odd. If g(x) has (x+1) as a factor, then g(1) =0 and all code words have an even number of 1s.

5. **Error bursts of length b: 0000110……0001101100….0**

Error pattern d(x)

e(x) =x^jd(x) where deg(d(x)) =L-1

g(x) has degree n-k;

g(x) cannot divide d(x) if deg(g(x))>deg(d(x))

**L=(n-k) or less : all errors will be detected.*

**L=(n-k+1): deg(d(x))=deg(g(x))*

i.e. d(x) =g(x) is the only undetectable error pattern fraction of bursts which are undetectable =1/2^{L-2}

** L> (n-k+1) : fraction of bursts which are undetectable=1/2^{n-k}*

Basic ARQ with CRC

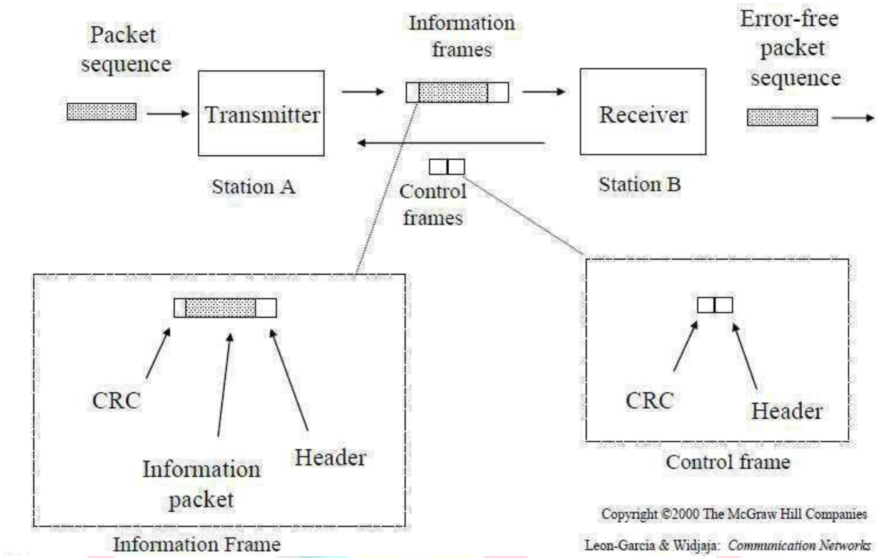


Fig. 5.15

The last error detection method we discuss here is called the checksum. The checksum is used in the Internet by several protocols although not at the data link layer. However, we briefly discuss it here to complete our discussion on error checking

Suppose our data is a list of five 4-bit numbers that we want to send to a destination. In addition to sending these numbers, we send the sum of the numbers. For example, if the set of numbers is (7, 11, 12, 0, 6), we send (7, 11, 12, 0, 6, 36), where 36 is the sum of the original numbers. The receiver adds the five numbers and compares the result with the sum. If the two are the same, the receiver assumes no error, accepts the five numbers, and discards the sum. Otherwise, there is an error somewhere and the data are not accepted.

We can make the job of the receiver easier if we send the negative (complement) of the sum, called the checksum. In this case, we send (7, 11, 12, 0, 6, −36). The receiver can add all the numbers received (including the checksum). If the result is 0, it assumes no error; otherwise, there is an error.

How can we represent the number 21 in one's complement arithmetic using only four bits?

Solution

The number 21 in binary is 10101 (it needs five bits). We can wrap the leftmost bit and add it to the four rightmost bits. We have (0101 + 1) = 0110 or 6.

How can we represent the number −6 in one's complement arithmetic using only four bits?
Solution

In one's complement arithmetic, the negative or complement of a number is found by inverting all bits. Positive 6 is 0110; negative 6 is 1001. If we consider only unsigned numbers, this is 9. In other words, the complement of 6 is 9. Another way to find the complement of a number in one's complement arithmetic is to subtract the number from $2^n - 1$ (16 − 1 in this case).

Let us redo using one's complement arithmetic.shows the process at the sender and at the receiver. The sender initializes the checksum to 0 and adds all data items and the checksum (the checksum is considered as one data item and is shown in color). The result is 36. However, 36 cannot be expressed in 4 bits. The extra two bits are wrapped and added with the sum to create the wrapped sum value 6. The sum is then complemented, resulting in the checksum value 9 (15 − 6 = 9). The sender now sends six data items to the receiver including the checksum 9.

The receiver follows the same procedure as the sender. It adds all data items (including the checksum); the result is 45. The sum is wrapped and becomes 15. The wrapped sum is complemented and becomes 0. Since the value of the checksum is 0, this means that the data is not corrupted. The receiver drops the checksum and keeps the other data items. If the checksum is not zero, the entire packet is dropped.

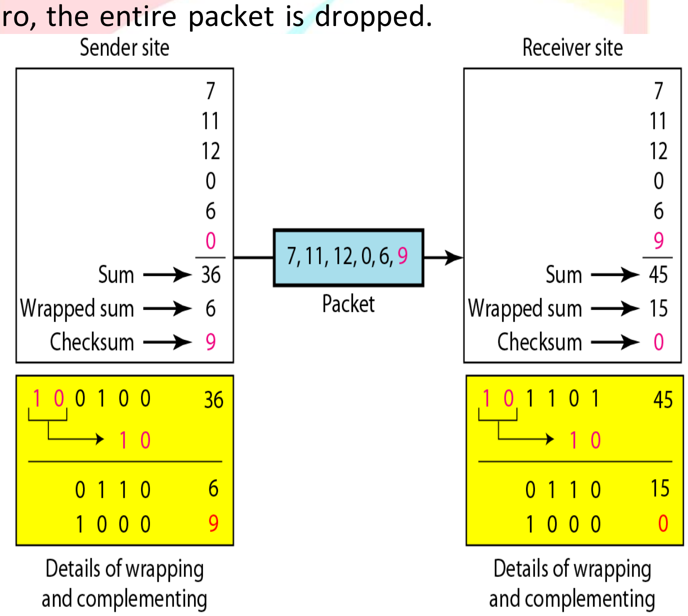


Fig. 5.16

Sender site:

1. The message is divided into 16-bit words.
2. The value of the checksum word is set to 0.
3. All words including the checksum are added using one's complement addition.
4. The sum is complemented and becomes the checksum.
5. The checksum is sent with the data.

Receiver site:

1. The message (including checksum) is divided into 16-bit words.

2. All words are added using one's complement addition.
3. The sum is complemented and becomes the new checksum.
4. If the value of checksum is 0, the message is accepted; otherwise, it is rejected.

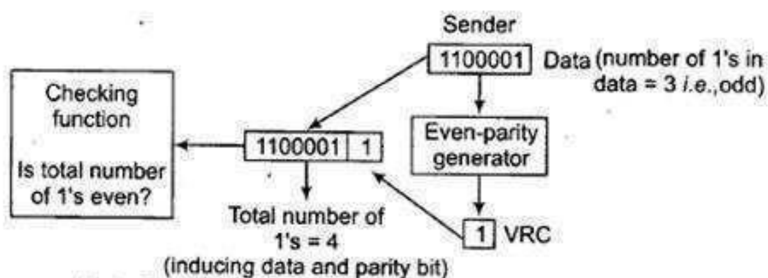
Let us calculate the checksum for a text of 8 characters ("Forouzan"). The text needs to be divided into 2-byte (16-bit) words. We use ASCII to change each byte to a 2 -digit hexadecimal number. For example, F is represented as 0x46 and o is represented as 0x6F. Figure below mentioned shows how the checksum is calculated at the sender and receiver sites. In part a of the figure, the value of partial sum for the first column is 0x36. We keep the rightmost digit (6) and insert the leftmost digit (3) as the carry in the second column. The process is repeated for each column. Note that if there is any corruption, the checksum recalculated by the receiver is not all 0s.

- Reliable systems must have mechanism for detecting and correcting such errors.
- Error detection and correction are implemented either at the data link layer or the transport layer of the OSI model.

Note: Checking function performs the action that the received bit stream passes the checking criteria, the data portion of the data unit is accepted else rejected.

Vertical Redundancy Check (VRC)

In this technique, a redundant bit, called parity bit, is appended to every data unit, so that the total number of 1's in the unit (including the parity bit) becomes even. If number of 1's are already even in data, then parity bit will be 0.

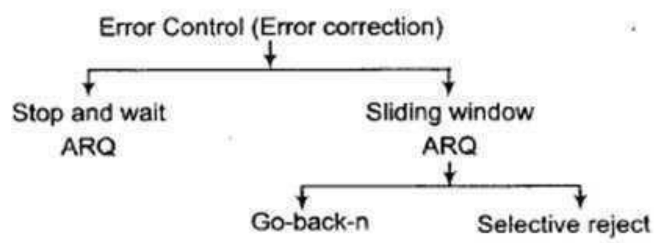


Detection of error using vertical redundancy check method

Fig. 5.17

Some systems may use odd parity checking, where the number of 1's should be odd. The principle is the same, the calculation is different.

Error Correction: Error correction in data link layer is implemented simply anytime, an error is detected in an exchange, a negative acknowledgement NAK is returned and the specified frames are retransmitted. This process is called Automatic Repeat Request (ARQ). Retransmission of data happens in three Cases: Damaged frame, Lost frame and Lost acknowledgement.



Error correction classification

Fig. 5.18

Convolutional Codes

Class of linear forward error correction (FEC) codes
Use convolution to encode data sequences
Encoders are usually binary digital filters
Coding rate R = k / n where k input symbols and n is output symbols.
Structure allows for much flexibility
Convolutional codes operate on streams of data
Linear block codes assume fixed-length messages
Lower encoding and decoding complexity than linear block codes for same coding rates.
Convolutional encoders are binary digital filters
FIR filters are called feedforward encoders
IIR filters are called feedback encoders

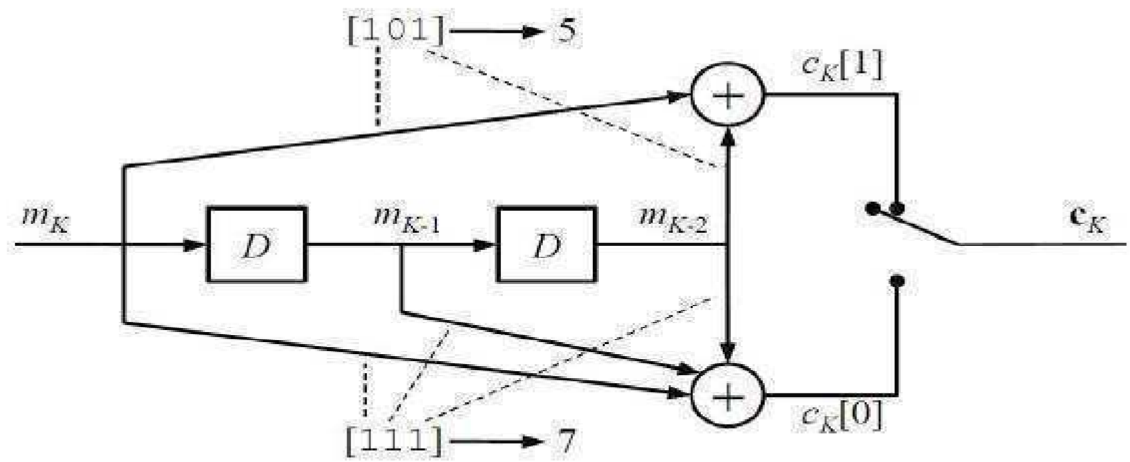


Fig. 5.19

A convolutional encoder can be thought of as a state machine
Current memory state and input affect output
Visualized in a state diagram

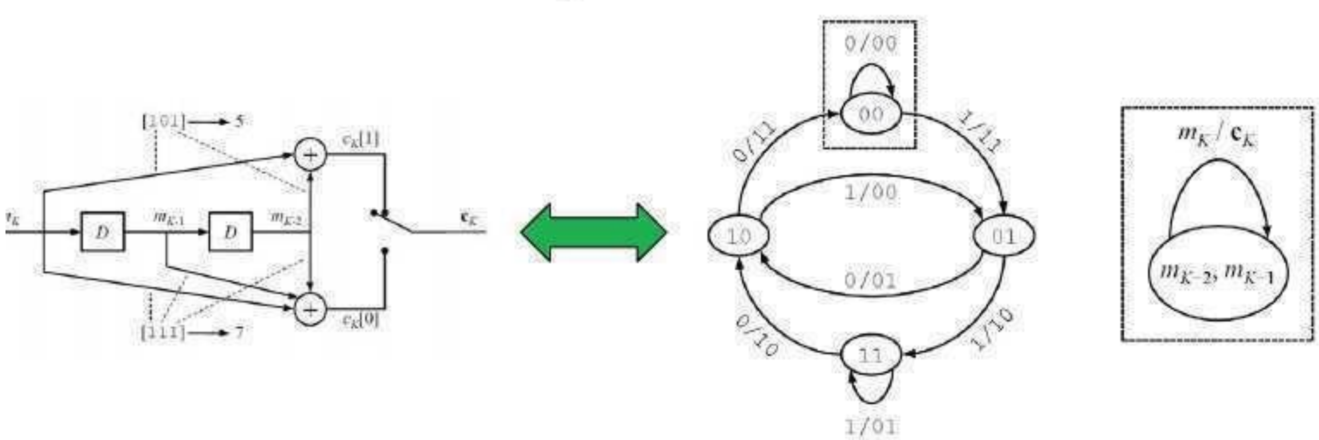


Fig. 5.20

Another representation is the trellis diagram

1. State diagram shown over time
2. Heavily used in many decoding algorithms
3. Viterbi algorithm
4. Soft output Viterbi algorithm
5. Others

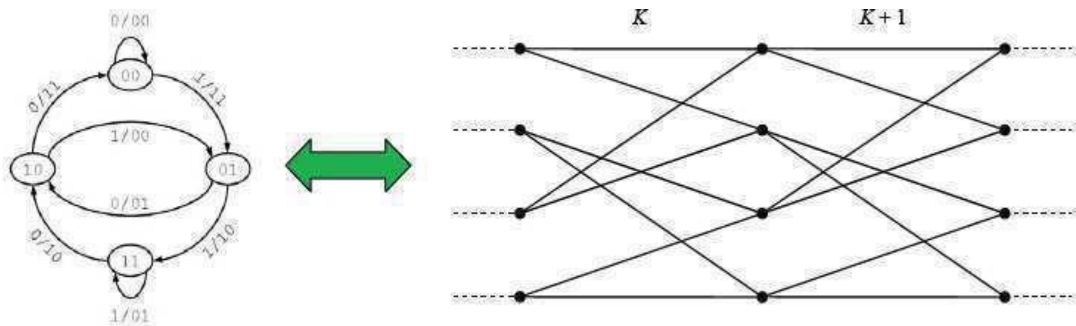


Fig. 5.21

Error Control: Error control in the data link layer is based on ARQ (automatic repeat request), which is the retransmission of data.

- The term error control refers to methods of error detection and retransmission.
- Anytime an error is detected in an exchange, specified frames are retransmitted. This process is called ARQ.

To ensure reliable communication, there needs to exist flow control (managing the amount of data the sender sends), and error control (that data arrives at the destination error free).

- Flow and error control needs to be done at several layers.
- For node-to-node links, flow and error control is carried out in the data-link layer.
- For end-point to end-point, flow and error control is carried out in the transport layer.

Flow & Error control:

- Error Detection and ARQ (error detection with retransmissions) must be combined with methods that intelligently limit the number of 'outstanding' (unACKed) frames.
- Flow & Error control techniques: Stop-and-Wait ARQ, Go-Back-N ARQ, and Selective Repeat ARQ

Flow Control Techniques:

- One important aspect of data link layer is flow control.
- Flow control refers to a set of procedures used to restrict the amount of data the sender can send before waiting for acknowledgement.

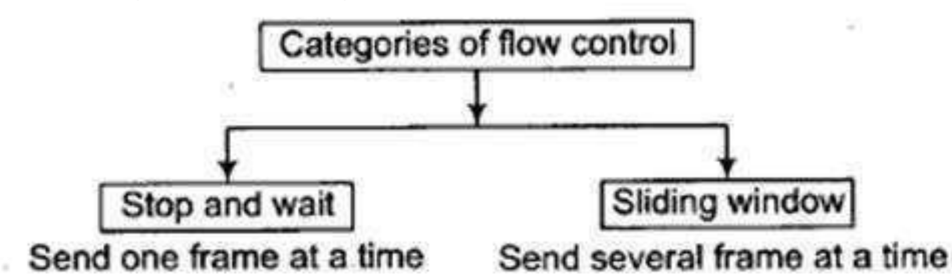


Fig. 5.22

Stop and Wait Flow control:

- The sender has to wait for an acknowledgment of every frame that it sends.

- Only when a acknowledgment has been received is the next frame sent. This process continues until the sender transmits an End of Transmission (EOT) frame.
- In Stop-and-Wait flow control, the receiver indicates its readiness to receive data for each frame.

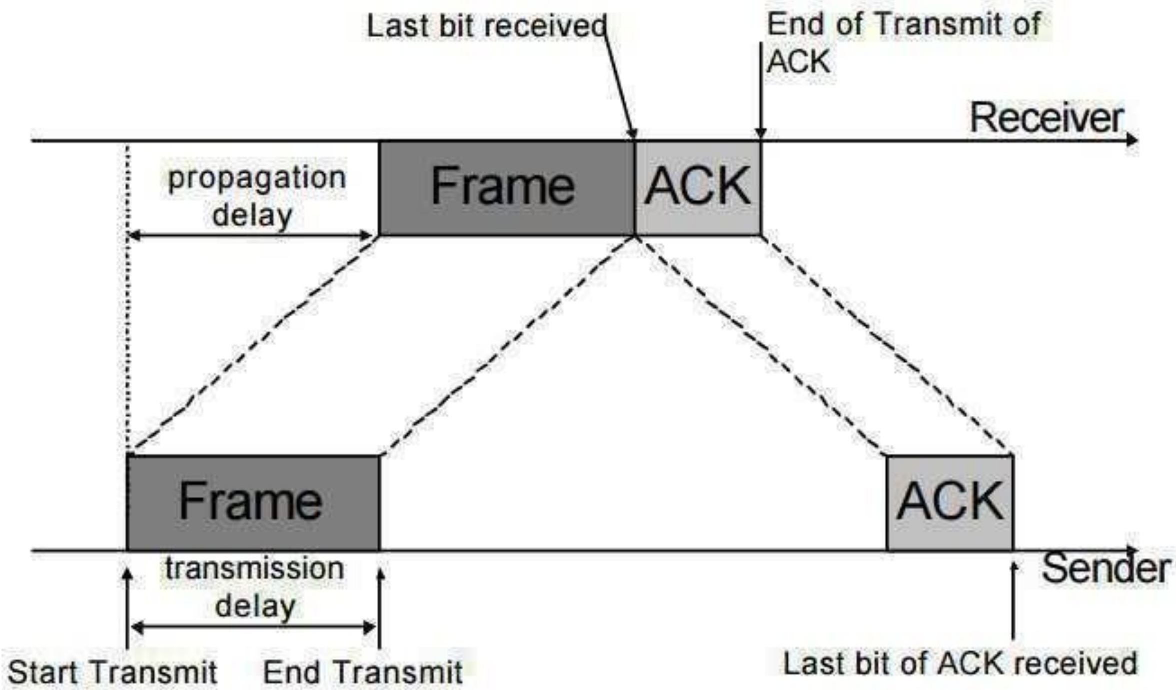


Fig. 5.23

1. For every frame that is sent, there needs to be an acknowledgment, which takes a similar amount of propagation time to get back to the sender.
2. Only one frame can be in transmission at a time. This leads to inefficiency if propagation delay is much longer than the transmission delay

Advantages of Stop and Wait:
It's simple and each frame is checked and acknowledged well.

Disadvantages of Stop and Wait:
1. Only one frame can be in transmission at a time.
2. It is inefficient, if the distance between devices is long. Reason is propagation delay is much longer than the transmission delay.
3. The time spent for waiting acknowledgements between each frame can add significant amount to the total transmission time.

Flow and Error Control Techniques (ARQ schemes):

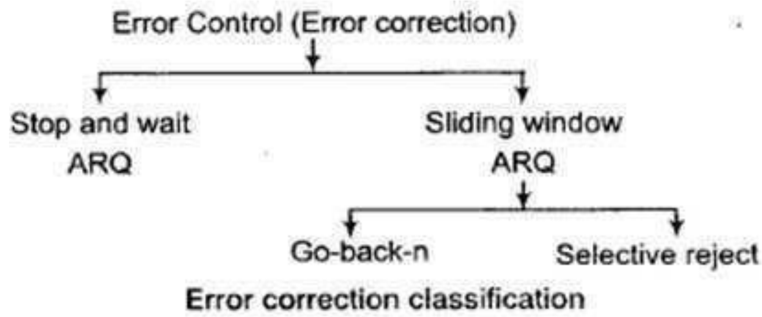


Fig. 5.24

Stop and Wait ARQ:

- Include re-transmission of data in case of lost or damaged framer.
- It is addition to the basic flow control mechanism with re-transmissions.
- (i) Sender sends an information frame to receiver.
- (ii) Sender waits for an ACK before sending the next frame.
- (iii) Receiver sends an ACK if frame is correctly received.
- (iv) If no ACK arrives within time-out, sender will resend the frame.

Time-out period >Rround trip time

- If an error is discovered in a data frame, indicating that it has been corrupted in transit, a NAK frame is returned. NAK frames, which are numbered, tell the sender to retransmit the last frame sent.
- **Piggybacking:** In bidirectional communications, both parties send & acknowledge data, i.e. both parties implement flow control. Outstanding ACKs are placed in the header of information frames, piggybacking can save bandwidth since the overhead from a data frame and an ACK frame (addresses, CRC, etc) can be combined into just one frame.

Sliding Window ARQ:

- To cover retransmission of lost or damaged frames, some features are added to the basic flow control mechanism of sliding window.
- A Sender may send multiple frames as allowed by the window size.
- The sending device keeps copies of all transmitted frames, until they have been acknowledged. .
- In addition to ACK frames, the receiver has the option of returning a NAK frame, if the data have been received damaged. NAK frame tells the sender to retransmit a damaged frame.
- Here, both ACK and NAK frames must be numbered for identification.
- ACK frames carry the number of next frame expected.
- NAK frames on the other hand, carry the number of the damaged frame itself.
- If the last ACK was numbered 3, an ACK 6 acknowledges the receipt of frames 3, 4 and 5 as well.
- If data frames 4 and 5 are received damaged, both NAK 4 and NAK 5 must be returned.
- Like stop and wait ARQ, the sending device in sliding window ARQ is equipped with a timer to enable it to handle lost acknowledgements.
- Sliding window ARQ is two types: Go-back-n ARQ, and Selective Reject ARQ.
- There are two ACK processing methods in sliding windows:
- Selective ACK: The **ACK N** message acknowledges **only** the frame with sequence number **N**

- Cumulative ACK : The **ACK N** message acknowledges **all** frames with sequence number **<= N**

(i) Go-back-n ARQ:

- The sliding window method using **cumulative ACK** is known as the **Go-Back-N** ARQ protocol.
- Receiver window size is 1.
- In this method, if one frame is lost or damaged all frames sent, since the last frame acknowledged are retransmitted.
- For example, sender may send frames 1,2,3,4 and get an NAK with a value of 2. The NAK acknowledges everything that came before it, and asks for frame 2 (and subsequent frames) to be resent.
- NAK number refer to the next expected frame number.
- Example: In the following figure, frame 2 has an error, then all subsequent frames are discarded. After timeout sender sends all frames from frame 2.

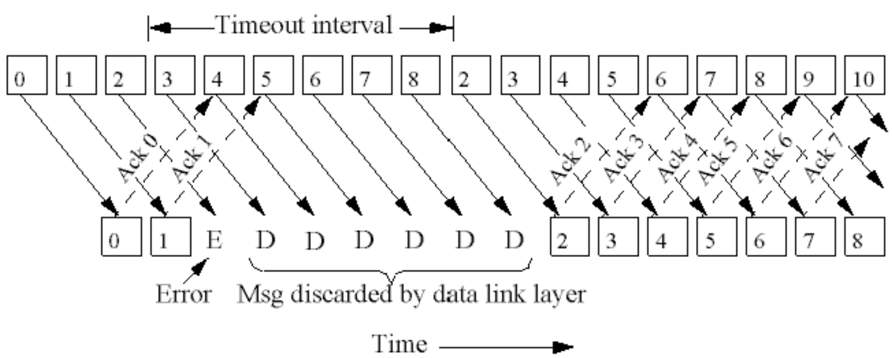


Fig. 5.25

Damaged/Error Frame :

1. In go-back-n ARQ, The receiver sends the NAK for this frame along with that frame number, that it expects to be retransmitted.
2. After sending NAK, the receiver discards all the frames that it receives, after a damagedframe.
3. The receiver does not send any ACK (acknowledgement) for the discarded frames. After the sender receives the NAK for the damaged frame, it retransmits all the framesonwards the frame number referred by NAK.

Lost frame:

1. In go-back-n ARQ, Receiver easily detects the loss of a frame as the newly received frame is received out of sequence.
2. The receiver sends the NAK for the lost frame and then the receiver discards all the frames received after a lost frame.
3. The receiver does not send any ACK for that discarded frames.
4. After the sender receives the NAK for the lost frame, it retransmits the lost frame referred by NAK and also retransmits all the frames which it has sent after the lost frame.

Lost Acknowledgement :

1. In go-back-n ARQ, If the sender does not receive any ACK or if the ACK is lost or damaged in between the transmission.
2. The sender waits for the time to run out and as the time run outs, the sender retransmits all the frames for which it has not received the ACK.
3. The sender identifies the loss of ACK with the help of a timer.
4. The ACK number, like NAK number, shows the number of the frame, that receiver expects to be the next in sequence.
5. The window size of the receiver is 1 as the data link layer only require the frame which it has to send next to the network layer.
6. The sender window size is equal to 'w'. If the error rate is high, a lot of bandwidth is lost wasted.

(ii) Selective Reject ARQ:

Selective Repeat ARQ overcomes the limitations of Go-Back-N by adding two new features:
Receiver window > 1 frame: Out-of-order but error-free frames can be accepted
Retransmission mechanism is modified: Only individual frames are retransmitted

1. In this method, only specific damaged or lost frame is retransmitted
2. Sender only retransmits frames for which a NAK is received.
3. NAK number refer to the frame lost.
4. If a frame is corrupted in transmit, a NAK is returned and the frame is resent out of sequence.
5. The sender needs to maintain all data that hasn't been aknowledged yet.
6. The receiving device must be able to sort the frames it has and insert the retransmitted frame into its proper place in the sequence.
7. It has advantage that few re-transmissions than go-back-n. But complexity at sender and receiver is involved.
8. Example: Frame 2 has an error, so receiver maintains buffer to store the next frames.

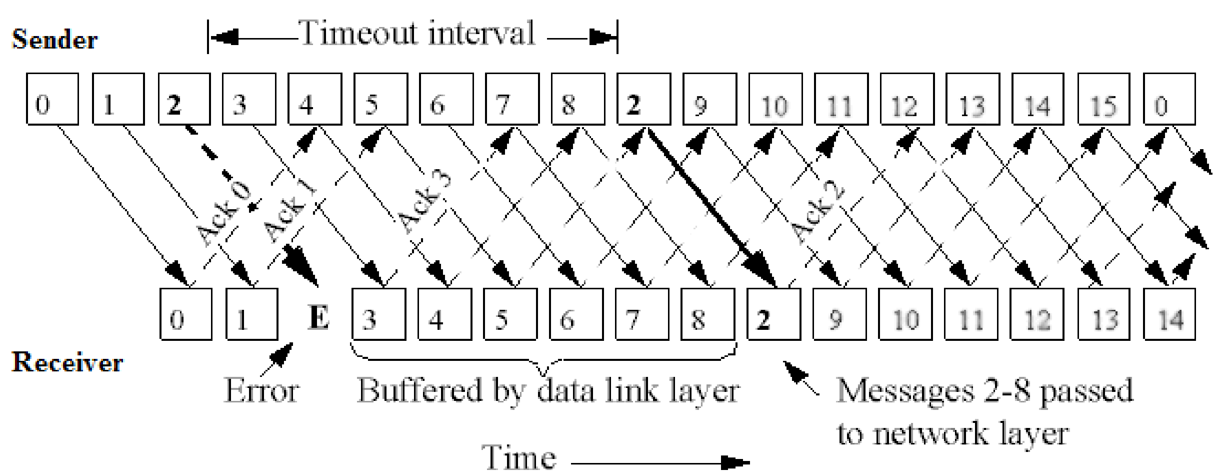


Fig. 5.26

Damaged frames :

1. In Selective reject, If a receiver receives a damaged frame, it sends the NAK for the frame in which error or damage is detected.

2. The NAK number, like in go-back-n also indicate the acknowledgement of the previously received frames and error in the current frame.
3. The receiver keeps receiving the new frames while waiting for the damaged frame to be replaced.
4. The frames that are received after the damaged frame are not be acknowledged until the damaged frame has been replaced.

Lost Frame :

1. As in a selective repeat protocol, a frame can be received out of order and further they are sorted to maintain a proper sequence of the frames.
2. While sorting, if a frame number is skipped, the receiver recognise that a frame is lost and it sends NAK for that frame to the sender.
3. After receiving NAK for the lost frame the sender searches that frame in its window and retransmits that frame.
4. If the last transmitted frame is lost then receiver does not respond and this silence is a negative acknowledgement for the sender.

Lost Acknowledgement :

1. In Selective reject, If the sender does not receive any ACK or the ACK is lost or damaged in between the transmission.
2. The sender waits for the time to run out and as the time run outs, the sender retransmit all the frames for which it has not received the ACK.
3. The sender identifies the loss of ACK with the help of a timer.

Interleaving

Interleaving is frequently used in digital communication and storage systems to improve the performance of forward error correcting codes. Many communication channels are not memoryless: errors typically occur in bursts rather than independently. If the number of errors within a code word exceeds the error-correcting code's capability, it fails to recover the original code word. Interleaving ameliorates this problem by shuffling source symbols across several code words, thereby creating a more uniform distribution of errors. Therefore, interleaving is widely used for burst error-correction.

The analysis of modern iterated codes, like turbo codes and LDPC codes, typically assumes an independent distribution of errors.Systems using LDPC codes therefore typically employ additional interleaving across the symbols within a code word.

For turbo codes, an interleaver is an integral component and its proper design is crucial for good performance. The iterative decoding algorithm works best when there are not short cycles in the factor graph that represents the decoder; the interleaver is chosen to avoid short cycles.

Interleaver designs include:

1. rectangular (or uniform) interleavers (similar to the method using skip factors described above)
2. convolutional interleavers

3. random interleavers (where the interleaver is a known random permutation)

4. S-random interleaver (where the interleaver is a known random permutation with the constraint that no input symbols within distance S appear within a distance of S in the output).

5. Another possible construction is a contention-free quadratic permutation polynomial (QPP).It is used for example in the 3GPP Long Term Evolution mobile telecommunication standard.

6. In multi-carrier communication systems, interleaving across carriers may be employed to provide frequency diversity, e.g., to mitigate frequency-selective fading or narrowband interference.

Transmission without interleaving:

Error-free message: aaaabbbbccccddddeeeeffffgggg
Transmission with a burst error: aaaabbbbccc deeeeffffgggg

Here, each group of the same letter represents a 4-bit one-bit error-correcting codeword. The codewordcccc is altered in one bit and can be corrected, but the codeworddddd is altered in three bits, so either it cannot be decoded at all or it might be decoded incorrectly.

With interleaving:

Error-free code words: aaaabbbbccccddddeeeeffffgggg
Interleaved: abcdefgabcdefgabcdefgabcdefg
Transmission with a burst error: abcdefgabcd bcdefgabcdefg
Received code words after deinterleaving: aa_abbbbccccdddde_eef_ffg_gg

In each of the codewordsaaaa, eeee, ffff, gggg, only one bit is altered, so one -bit error-correcting code will decode everything correctly.

Transmission without interleaving:

Original transmitted sentence: ThisIsAnExampleOfInterleaving
Received sentence with a burst error: ThisIs ______ pleOfInterleaving

The term "AnExample" ends up mostly unintelligible and difficult to correct.

With interleaving:

Transmitted sentence: ThisIsAnExampleOfInterleaving...
Error-free transmission: TIEpfeaghsxlIrv.iAaenli.snmOten.
Received sentence with a burst error: TIEpfe ______ Irv.iAaenli.snmOten.
Received sentence after deinterleaving: T_isI_AnE_amp_eOfInterle_vin_...

No word is completely lost and the missing letters can be recovered with minimal guesswork.

Disadvantages of interleaving

Use of interleaving techniques increases total delay. This is because the entire interleaved block must be received before the packets can be decoded. Also interleavers hide the structure of errors; without an interleaver, more advanced decoding algorithms can take advantage of the error structure and achieve more reliable communication than a simpler decoder combined with an interleaver.

Video Links:-

1. nptel.ac.in/courses/106105082/16
2. http://freevideolectures.com/ Networking/ IIT Kharagpur