Subject:-Computer Networks
Subject code:- BCA 210

Unit - I

Basic Concepts: Components of data communication, distributed processing, Line configuration, topology, transmission mode, and categories of networks. OSI and TCP/IP Models: Layers and their functions, comparison of models. Digital Transmission: Interfaces and Modems: DTE-DCE Interface, modems, cable modems. Transmission Media: Guided and unguided, Attenuation, distortion, noise, throughput, propagation speed and time, wavelength, Shannon Capacity.

Unit – II

Telephony: Multiplexing, error detection and correction: Many to one, one to many, WDM, TDM, FDM, circuit switching, packet switching and message switching. Data Link control protocols: Line discipline, flow control, error control, synchronous and asynchronous protocols overview.

ISDN: Services, historical outline, subscriber's access, ISDN, Layers, and broadband ISDN.

Unit-III

Devices: Repeaters, bridges, gateways, routers, The Network Layer, Design Issues, Network Layer Addressing and Routing concepts (Forwarding Function, Filtering Function);Routing Methods (Static and dynamic routing, Distributed routing, Hierarchical Routing);Distance Vector Protocol, Link State protocol.

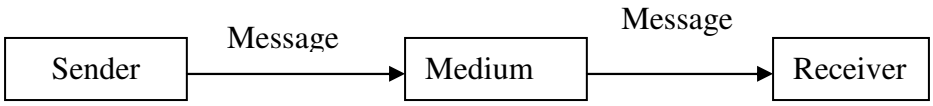
Unit – IV

Transport and upper layers in OSI Model: Transport layer functions, connection management, Functions of session layers, Presentation layer, and Application layer.

Unit - I

Basic Concepts: Components of data communication:

Communication: To convey any message, data or thoughts from one place to another place using some medium is termed as a communication.



Components of data communication:

1. Sender
2. Message
3. Medium
4. Receiver
5. Protocols
6. Feedback

Sender: Sender is the person who sends message.

Message: Message is the information that is exchanged between sender and receiver

Medium: Medium is the channel through which sender will communicate his message.

Receiver: The person to whom the message is being sent is called 'receiver'. Receiver is the person who interprets the message.

Protocols: Protocols are some set of rules followed by the sender and receiver for communication.

Feedback: Response or reaction of the receiver, to a message, is called 'feedback'. Feedback may be written or oral message, an action or simply, silence may also be a feedback to a message. Communication is said to be effective only when it receives some feedback. Feedback, actually, completes the loop of communication.

Distributed processing: *Distributed processing* accelerates processing by distributing the work to multiple computers that have been chosen to provide more processing power. Distributed processing is a phrase used to refer to a variety of computer systems that use more than one computer (or processor) to run an application.

Line configuration:

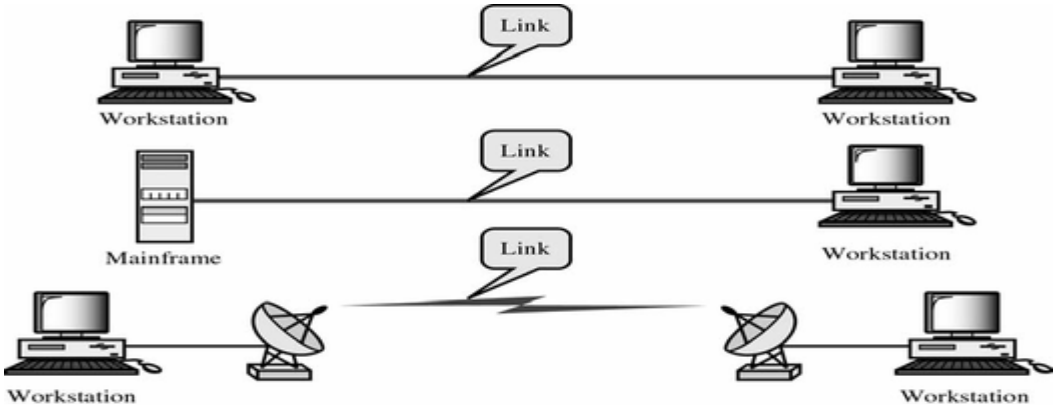
Line configuration refers to the way two or more communication devices attached to a link. Line configuration is also referred to as connection. A Link is the physical communication pathway that transfers data from one device to another. For communication to occur, two devices must be connected in same way to the same link at the same time.

Types of line configuration

1. Point-to-Point.
2. Multipoint.

Point-to-Point:

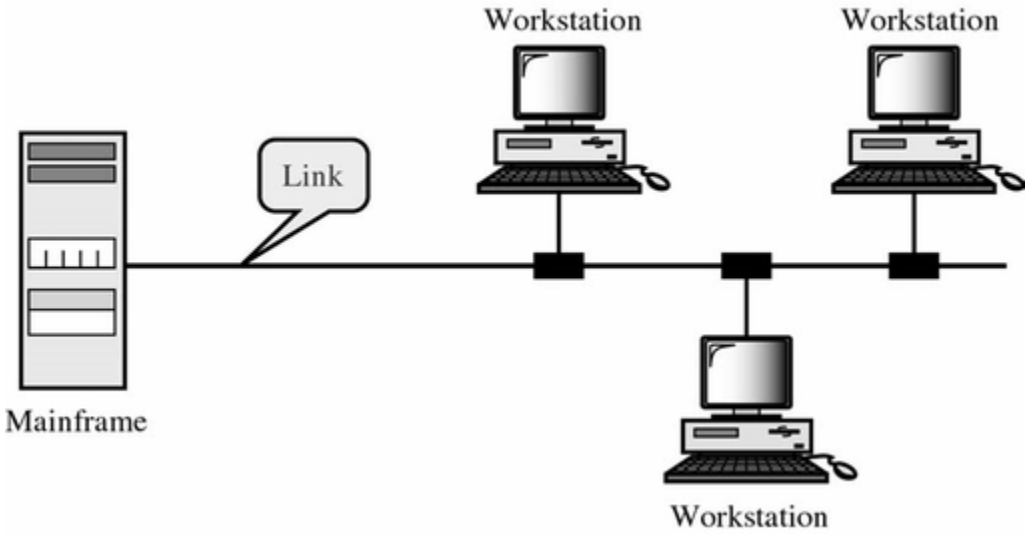
A Point to Point Line Configuration Provide dedicated link between two devices use actual length of wire or cable to connect the two end including microwave & satellite link. Infrared remote control.



Multipoint Configuration:

Multipoint Configuration also known as Multidrop line configuration one or more than two specific devices share a single link capacity of the channel is shared. With shared capacity, there can be two possibilities in a Multipoint Line Configuration:

- **Spatial Sharing**: If several devices can share the link simultaneously, it's called Spatially shared line configuration
- **Temporal (Time) Sharing**: If users must take turns using the link , then it's called Temporally shared or Time Shared Line Configuration



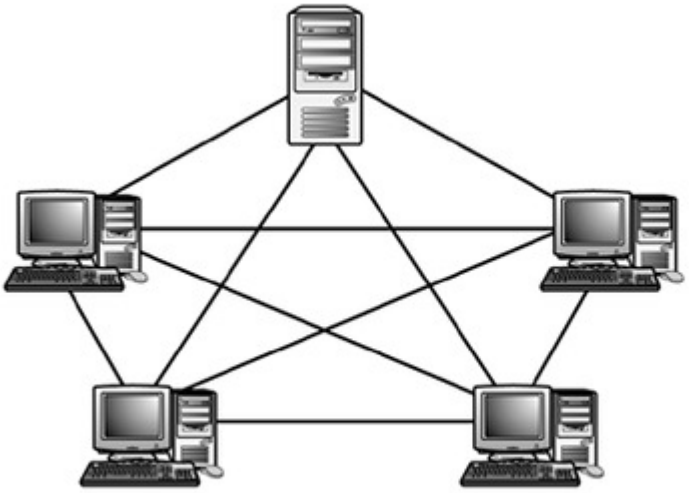
Topology:

The term "Topology" refers to the way in which the end points or stations/computer systems, attached to the networks, are interconnected. We have seen that a topology is essentially a stable geometric arrangement of computers in a network.

Types of topology:

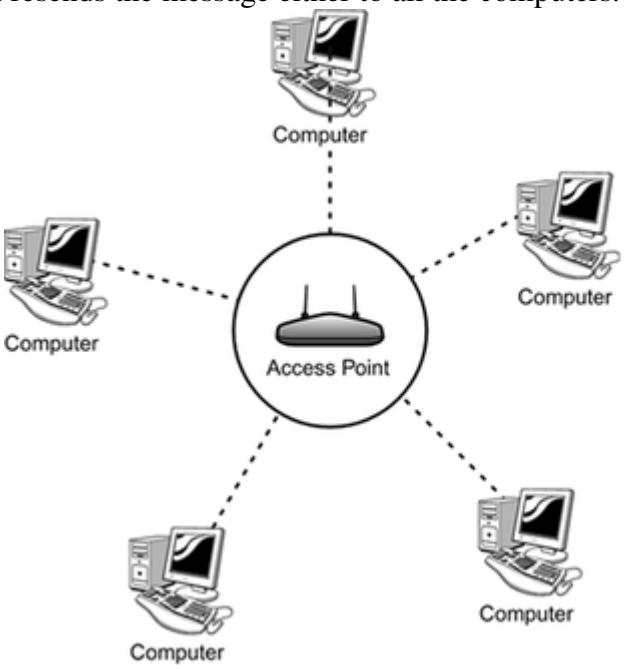
(1) Mesh topology.
(2) Star topology.
(3) Tree (Hierarchical) topology.
(4) Bus topology.
(5) Ring topology.

1. Mesh Topology: In mesh topology each node is connected to all other nodes. It is also called as fully connected mesh topology. The number of connections in a full mesh = n(n - 1) / 2



2. Star Topology:

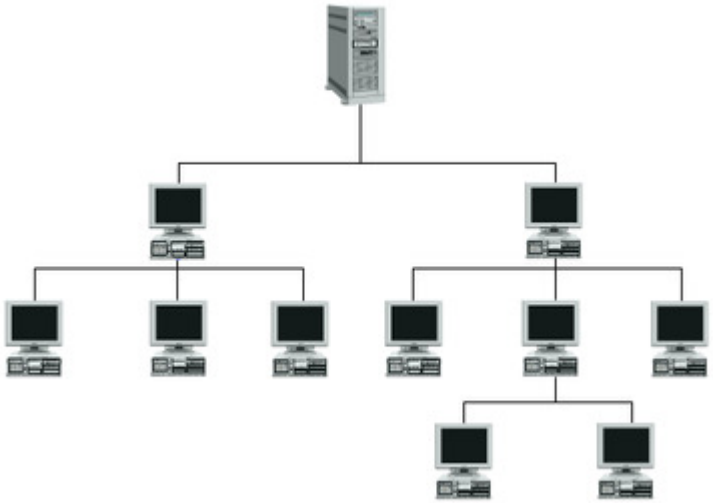
In a star topology, cables run from every computer to a centrally located device called a HUB. Star topology networks require a central point of connection between media segment. These central points are referred to as Hubs. Hubs are special repeaters that overcome the electromechanical limitations of a media. Each computer on a star network communicates with a central hub that resends the message either to all the computers.



3. Tree (Hierarchical) topology:

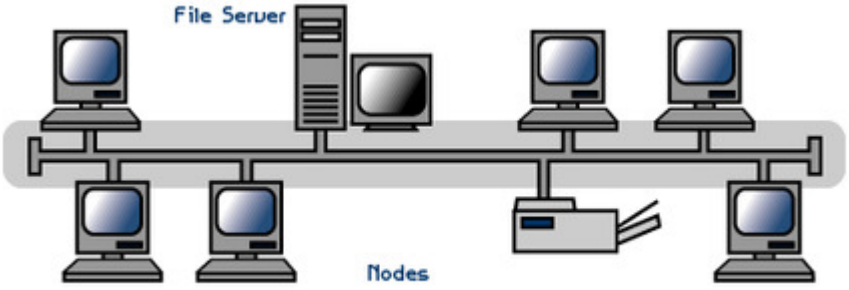
It is similar to the star network, but the nodes are connected to the secondary hub that in turn is connected to the central hub. The central hub is the active hub. The active hub contains the

repeater, which regenerates the bits pattern it receives before sending them out. The secondary hub can be either active or passive. A passive hub provides a simple physical connection between the attached devices.



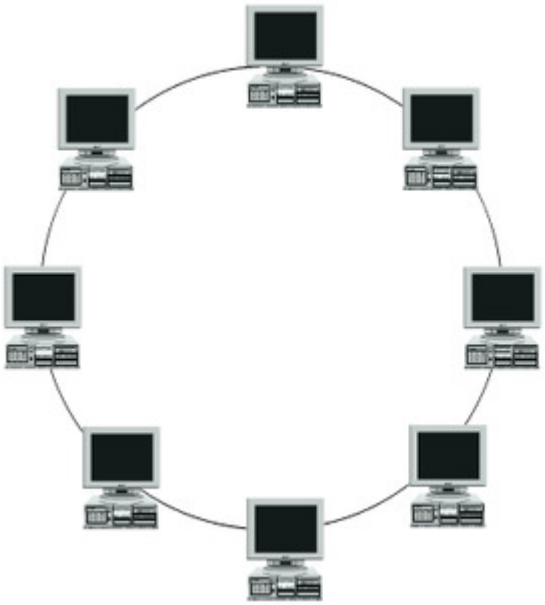
4. Bus topology:

A bus topology connects computers along a single or more cable to connect linearly. A network that uses a bus topology is referred to as a "bus network" which was the original form of Ethernet networks. Ethernet 10Base2 (also known as thinnet) is used for bus topology.



5. Ring topology:

In ring topology, each device has a dedicated point-to-point line configuration only with two devices on either side of it. A signal is passed along the ring in one direction, from device to device until it reaches its destination. Each device in the ring has a repeater. When the devices receive the signal intended for the other node, it just regenerates the bits and passes them along. Ring network passes a token. A token is a short message with the electronic address of the receiver. Each network interface card is given a unique electronic address, which is used to identify the computer on the network.



Transmission mode:

A given transmission on a communications channel between two machines can occur in several different ways.

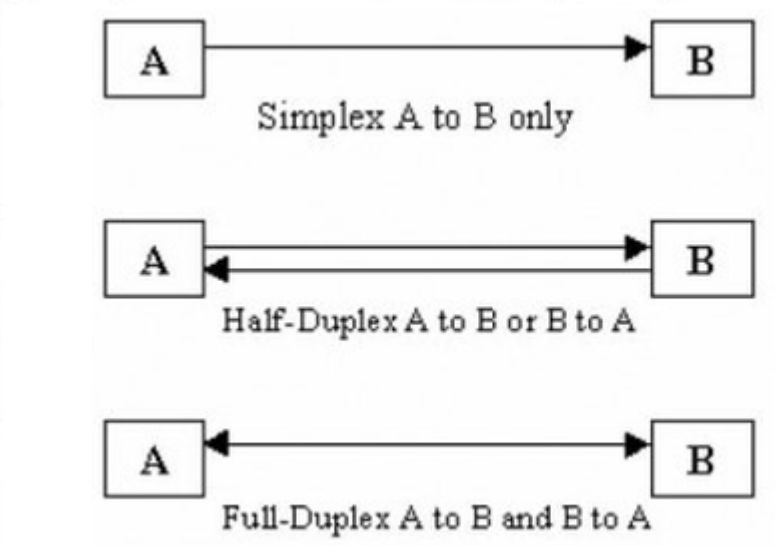
Types of Transmission mode

- Simplex
- Half Duplex
- Full Duplex

A simplex connection is a connection in which the data flows in only one direction, from the transmitter to the receiver. This type of connection is useful if the data do not need to flow in both directions (for example, from your computer to the printer or from the mouse to your computer...).

A half-duplex connection (sometimes called an *alternating connection* or *semi-duplex*) is a connection in which the data flows in one direction or the other, but not both at the same time. With this type of connection, each end of the connection transmits in turn. This type of connection makes it possible to have bidirectional communications using the full capacity of the line.

A full-duplex connection is a connection in which the data flow in both directions simultaneously. Each end of the line can thus transmit and receive at the same time, which means that the bandwidth is divided in two for each direction of data transmission if the same transmission medium is used for both directions of transmission.

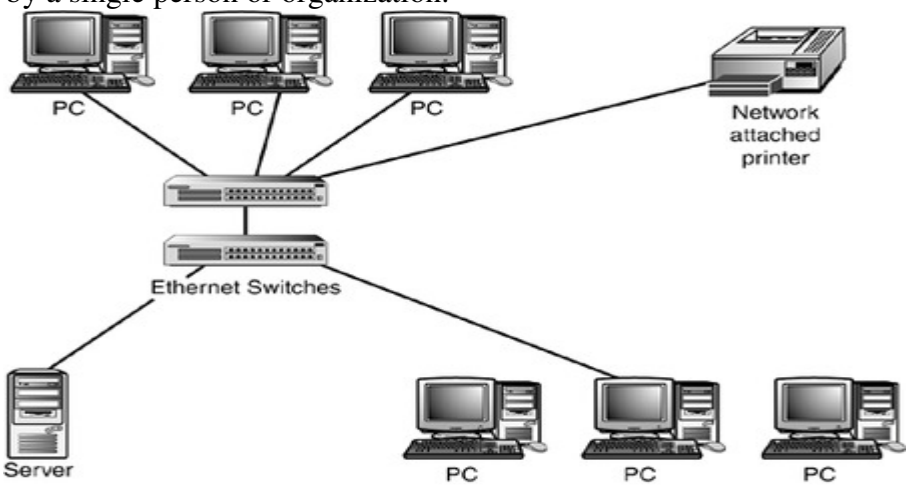


Categories of networks:

- LAN - Local Area Network
- MAN - Metropolitan Area Network
- WAN - Wide Area Network

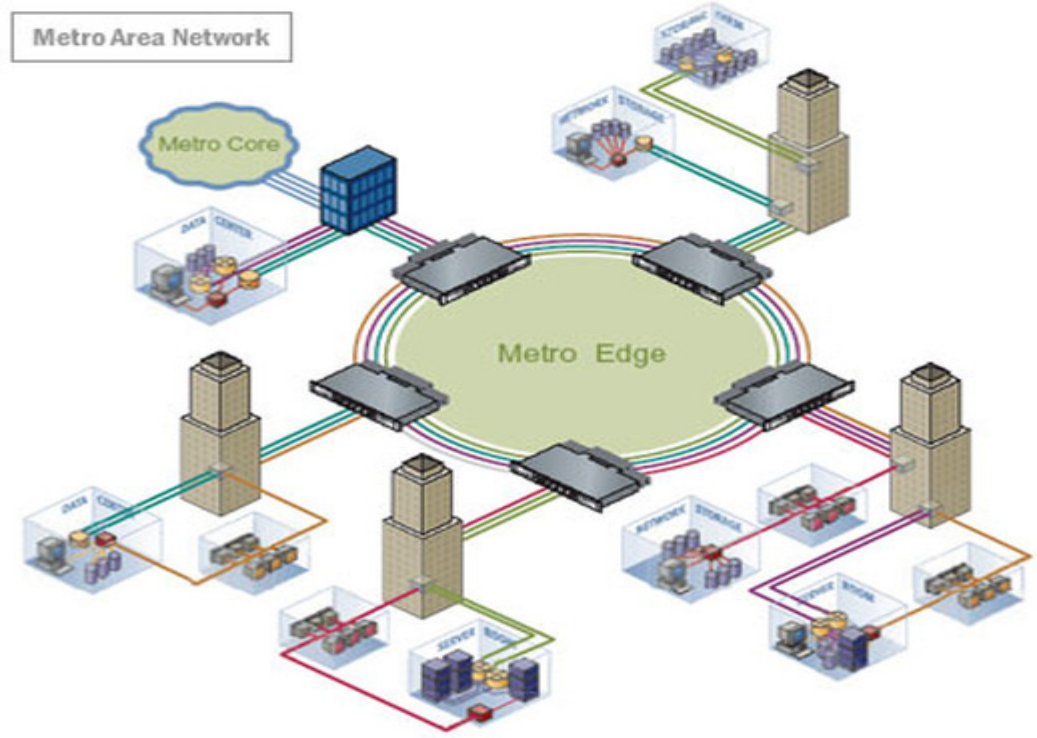
Local Area Network:

A LAN connects network devices over a relatively short distance. A networked office building, school, or home usually contains a single LAN, though sometimes one building will contain a few small LANs (perhaps one per room), and occasionally a LAN will span a group of nearby buildings. In addition to operating in a limited space, LANs are also typically owned, controlled, and managed by a single person or organization.



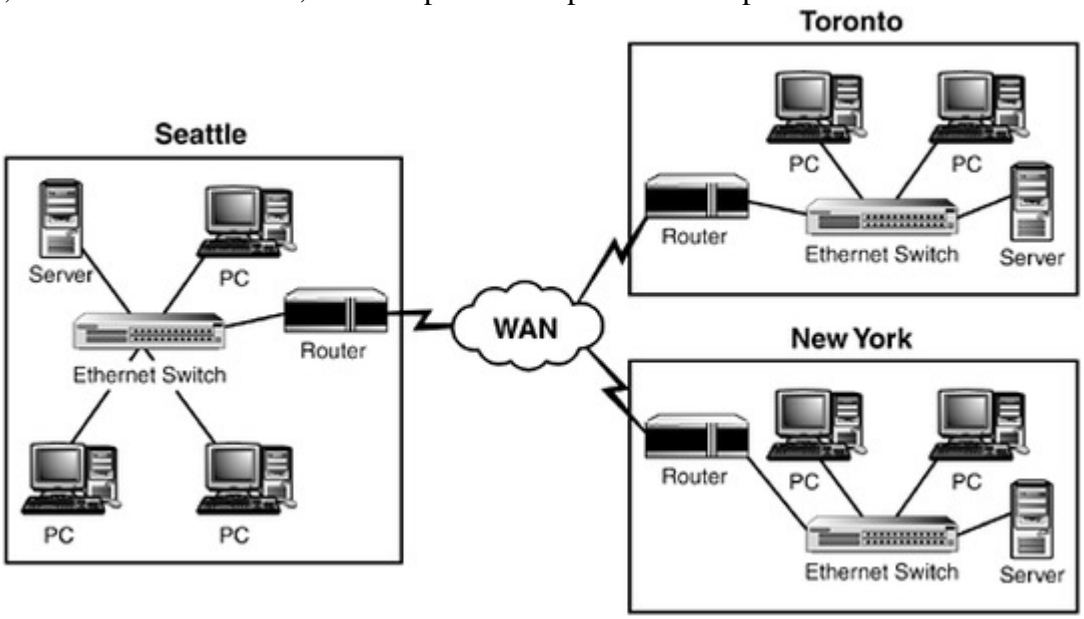
Metropolitan Area Network:

Any network spreading over a physical area larger than a LAN but smaller than a WAN, such as a city. A MAN is typically owned and operated by a single entity such as a government body or large corporation.



Wide Area Network:

A WAN is a network that spans more than one geographical location often connecting separated LANs. WANs are slower than LANs and often require additional and costly hardware such as routers, dedicated leased lines, and complicated implementation procedures.



OSI and TCP/IP Models: Layers and their functions:

1. Physical layer
2. Data Link layer
3. Network layer
4. Transport layer
5. Session layer
6. Presentation layer
7. Application layer

Physical layer:

- Establishment and termination of a connection to a communications medium.
- Participation in the process whereby the communication resources are effectively shared among multiple users. For example, contention resolution and flow control.
- Modulation or conversion between the representation of digital data in user equipment and the corresponding signals transmitted over a communications channel. These are signals operating over the physical cabling (such as copper and optical fiber) or over a radio link.

Data Link layer:

- Framing
- Physical Addressing
- Flow Control
- Error Control
- Access Control
- Media Access Control (MAC)

Network layer:

- Maintaining the quality of service requested by the transport layer.
- The network layer performs network routing functions, and might also perform fragmentation and reassembly, and report delivery errors.
- Routers operate at this layer, sending data throughout the extended network and making the Internet possible.

Transport layer:

- The transport layer provides transparent transfer of data between end users.
- It providing reliable data transfer services to the upper layers.
- The transport layer controls the reliability of a given link through flow control, segmentation/desegmentation, and error control.
- Some protocols are state- and connection-oriented. This means that the transport layer can keep track of the segments and retransmit those that fail.
- The transport layer also provides the acknowledgement of the successful data transmission and sends the next data if no errors occurred.

Session layer:

- The session layer controls the dialogues (connections) between computers.
- It establishes, manages and terminates the connections between the local and remote application.
- It provides for full-duplex, half-duplex, or simplex operation, and establishes checkpoint, adjournment, termination, and restart procedures.
- The OSI model made this layer responsible for graceful close of sessions, which is a property of the Transmission Control Protocol, and also for session checkpoint and recovery, which is not usually used in the Internet Protocol Suite.
- The session layer is commonly implemented explicitly in application environments that use remote procedure calls.

Presentation layer:

- The presentation layer establishes context between application-layer entities, in which the higher-layer entities may use different syntax and semantics if the presentation service provides a mapping between them. If a mapping is available, presentation service data units are encapsulated into session protocol data units, and passed down the stack.
- This layer provides independence from data representation (e.g., encryption) by translating between application and network formats.
- The presentation layer transforms data into the form that the application accepts.
- This layer formats and encrypts data to be sent across a network. It is sometimes called the syntax layer.

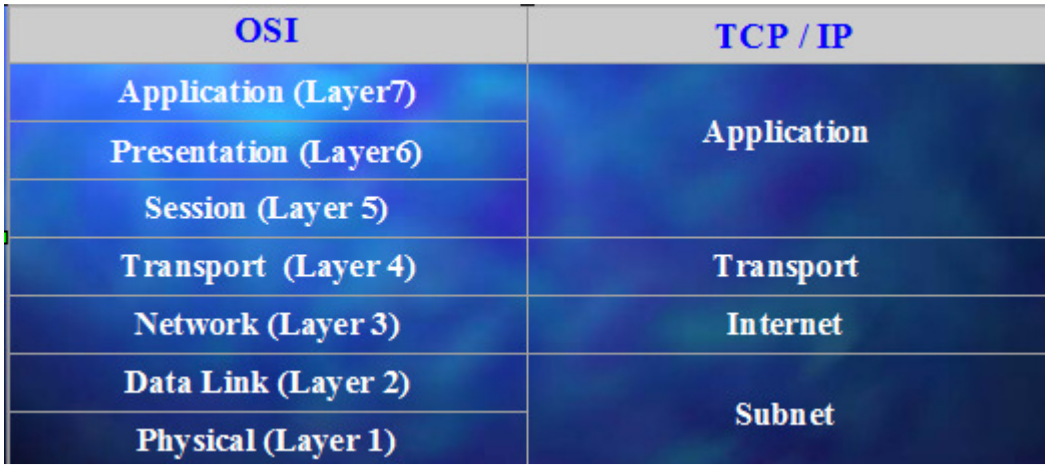
Application layer:

- The application layer is the OSI layer closest to the end user, which means that both the OSI application layer and the user interact directly with the software application.
- This layer interacts with software applications that implement a communicating component.
- Application-layer functions typically include identifying communication partners, determining resource availability, and synchronizing communication.
- When identifying communication partners, the application layer determines the identity and availability of communication partners for an application with data to transmit.
- When determining resource availability, the application layer must decide whether sufficient network or the requested communication exists.
- In synchronizing communication, all communication between applications requires cooperation that is managed by the application layer

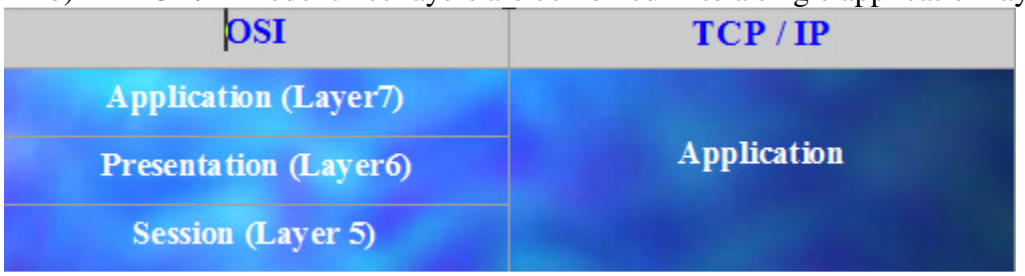
<u>Comparison of models:</u>

1. Open System Interconnection Model (OSI)
2. Transport Control Protocol /Internet Protocol (TCP/IP)

a) There are seven layers in OSI model where as TCP/IP has only five layers.



b) In TCP /IP model three layers are combined in to a single application layer.



c) The Session layer permits two parties to hold ongoing communications called a session across a network. Not found in TCP/IP model. In TCP/IP, its characteristics are provided by the TCP protocol.(Transport Layer)

d) The Presentation Layer handles data format information for networked communications. This is done by converting data into a generic format that could be understood by both sides. Not found in TCP/IP model. In TCP/IP, this function is provided by the Application Layer.
e.g. External Data Representation Standard (XDR) Multipurpose Internet Mail Extensions (MIME)

e) The Application Layer is the top layer of the reference model. It provides a set of interfaces for applications to obtain access to networked services as well as access to the kinds of network services that support applications directly.
OSI - FTAM,VT,MHS,DS,CMIP
TCP/IP - FTP,SMTP,TELNET,DNS,SNMP
Although the notion of an application process is common to both, their approaches to constructing application entities are different.

f) Like all the other OSI Layers, the network layer provides both connectionless and connection-oriented services. As for the TCP/IP architecture, the internet layer is exclusively connectionless.

g) Implementation of the OSI model places emphasis on providing a reliable data transfer service, while the TCP/IP model treats reliability as an end-to-end problem.

h) Each layer of the OSI model detects and handles errors, all data transmitted includes checksums. The transport layer of the OSI model checks source-to-destination reliability.

i) In the TCP/IP model, reliability control is concentrated at the transport layer. The transport layer handles all error detection and recovery. The TCP/IP transport layer uses checksums, acknowledgments, and timeouts to control transmissions and provides end-to-end verification.
j) Hosts on OSI implementations do not handle network operations (simple terminal), but TCP/IP hosts participate in most network protocols.
k) TCP/IP hosts carry out such functions as end-to-end verification, routing, and network control. The TCP/IP internet can be viewed as a data stream delivery system involving intelligent hosts.

Digital /Analog Transmission: Introduction

Analog Signals:

An **analog** or **analogue signal** is any continuous signal for which the time varying feature (variable) of the signal is a representation of some other time varying quantity, i.e., analogous to another time varying signal. It differs from a digital signal in terms of small fluctuations in the signal which are meaningful. Analog is usually thought of in an electrical context; however, mechanical, pneumatic, hydraulic, and other systems may also convey analog signals.

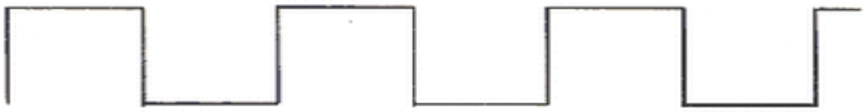
Digital Signals:

A **digital signal** is a chemical signal that is a representation of a sequence of discrete values (a quantified discrete-time signal), for example of arbitrary bit stream, or of a digitized (sampled and analog-to-digital converted) analog signal. The term digital signal can refer to

1. A continuous-time waveform signal used in any form of digital communication.
2. A pulse train signal that switches between a discrete number of voltage levels or levels of light intensity, also known as a a line coded signal, for example a signal found in digital electronics or in serial communications using digital baseband transmission in, or a pulse code modulation (PCM) representation of a digitized analog signal.

A signal that is generated by means of a digital modulation method (digital pass band transmission), produced by a modem, is in the first case considered as a digital signal, and in the second case as converted to an analog signal.

Analog Signal



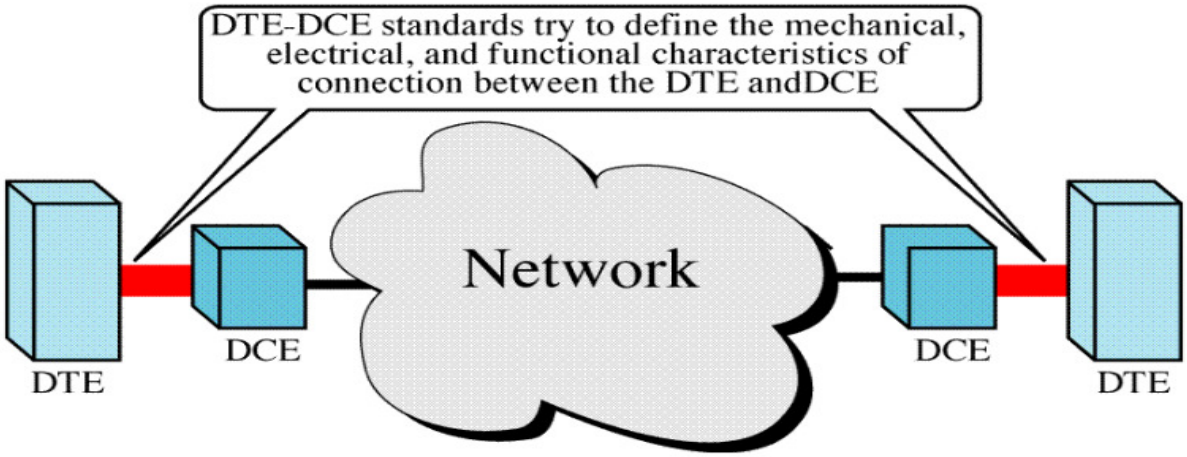
Digital Signal

Interfaces and Modems:

DTE-DCE Interface:

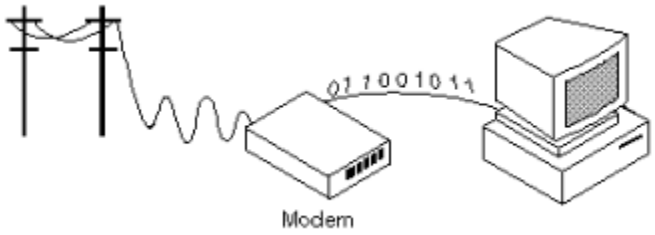
Data terminal equipment (**DTE**) is an end instrument that converts user information into signals or reconverts received signals. These can also be called tail circuits. A DTE device communicates with the data circuit-terminating equipment (DCE). It can be a terminal, computer, microcomputer, printer, fax machine or any other device that either generates or consumes digital data.

Data circuit-terminating equipment (DCE):
Any efficient component that either transmits or receives data and information in the structure of an analog or digital signal all the way through network. A DCE takes information generated by a DTE, changes them to a suitable signal, and then introduces the signal onto the telecommunication link.



Modems :

A **modem** (***mo****dulator-****dem****odulator*) is a device that modulates an analog signal to digital signals, and also demodulates such a signal to decode the transmitted information. The goal is to produce a signal that can be transmitted easily and decoded to reproduce the original digital data. Modems can be used with any means of transmitting analog signals.



Cable modems:

To access Internet through a Cable TV network, Computer Network requires a cable Modem. It has two interfaces on it one for computer and other for Cable Network. This Modem makes a connection when it is turned on. Cable modems are always retaining the connection (unless they are switched off) because the cable operator does not charge for the duration of connection.

When a cable Modem is switched on It scans the downstream channel looking for a special packet periodically (special packet contains the modem configuration and sender of this is the head end), after getting the packet, the new modem sends a packet on one of the upstream channel.

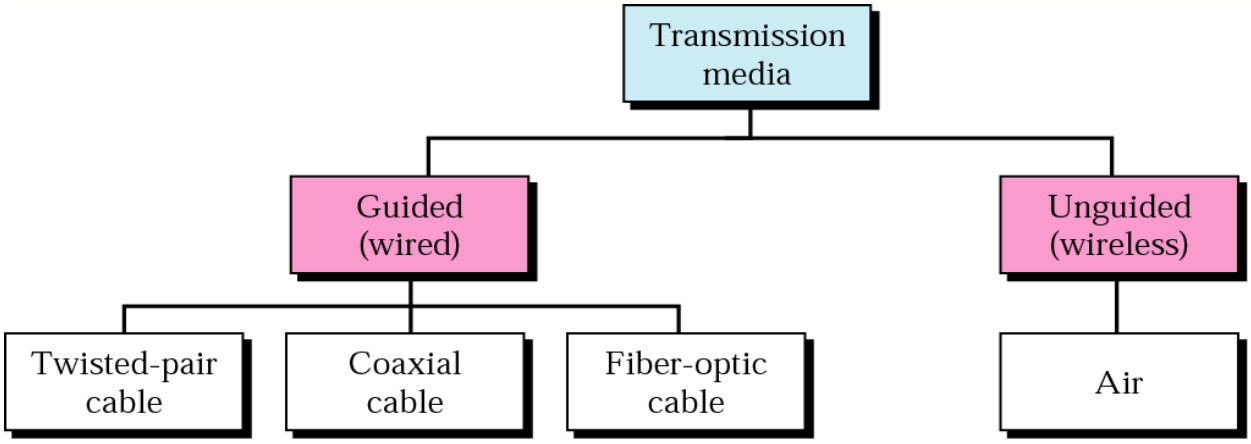
Transmission Media: Guided and unguided:

Transmission media means any medium used for communication. It can be divided into two categories':

1. Guided media
2. Unguided media

Guide media is that where we use any path for communication like cables (coaxial, fibre optic, twisted pair) etc. Examples of guided media are:- Twisted Pair Cable, Co-axial Cable, Optical Fiber Cable.

Unguided media is also called wireless where not any physical path is used for transmission. Examples of unguided media are:- Microwave or Radio Links, Infrared.



There are three categories of guided media:
Twisted-pair cable
Coaxial cable
Fiber-optic cable

Twisted pair consists of two conductors (normally copper), each with its own plastic insulation, twisted together.
Twisted-pair cable comes in two forms: unshielded and shielded
The twisting helps to reduce the interference (noise) and crosstalk.

Figure 7.4 *Frequency range for twisted-pair cable*

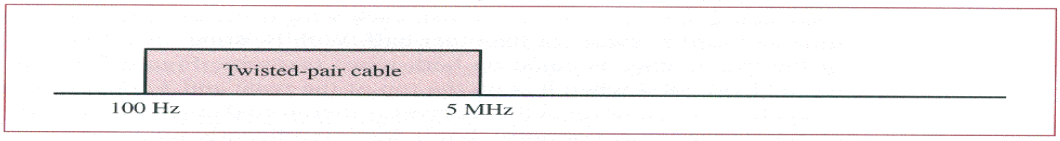
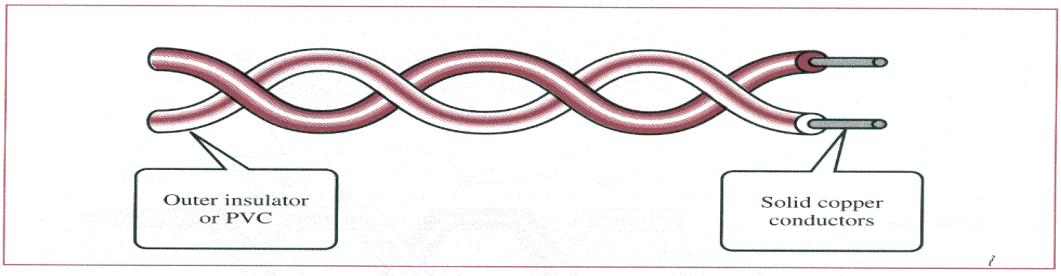
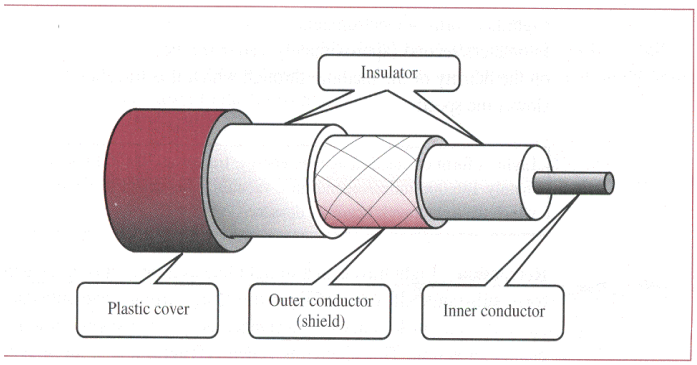


Figure 7.5 *Twisted-pair cable*



Coaxial cable carries signals of higher frequency ranges than twisted-pair cable. It has inner conductor ,Insulator, Outer conductor metal mesh, Insulator and plastic cover.

Figure 7.12 *Coaxial cable*

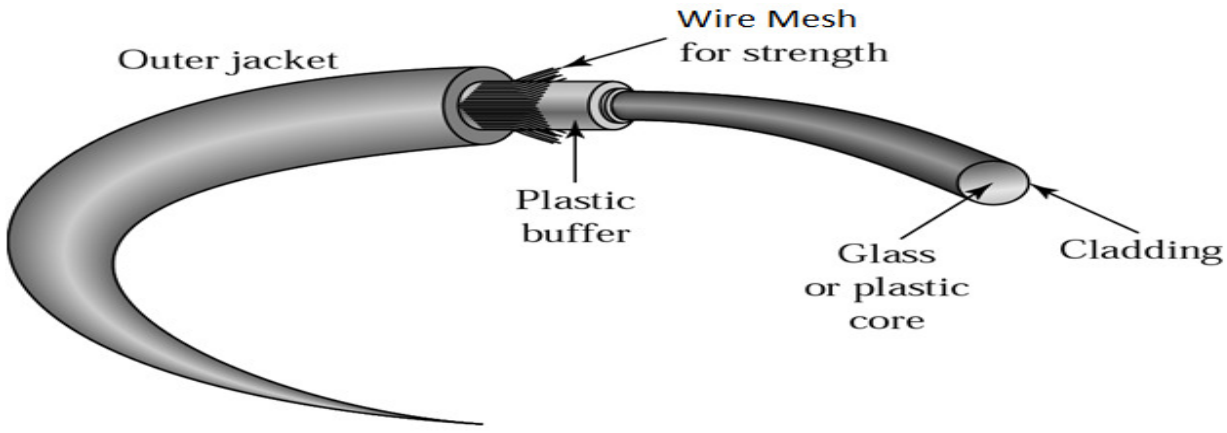


Applications:

- Television distribution
- Cable TV
- Long distance telephone transmission
- Can carry 10,000 voice calls simultaneously
- Short distance computer systems links
- Local area networks
- More expensive than twisted pair, not as popular for LANs

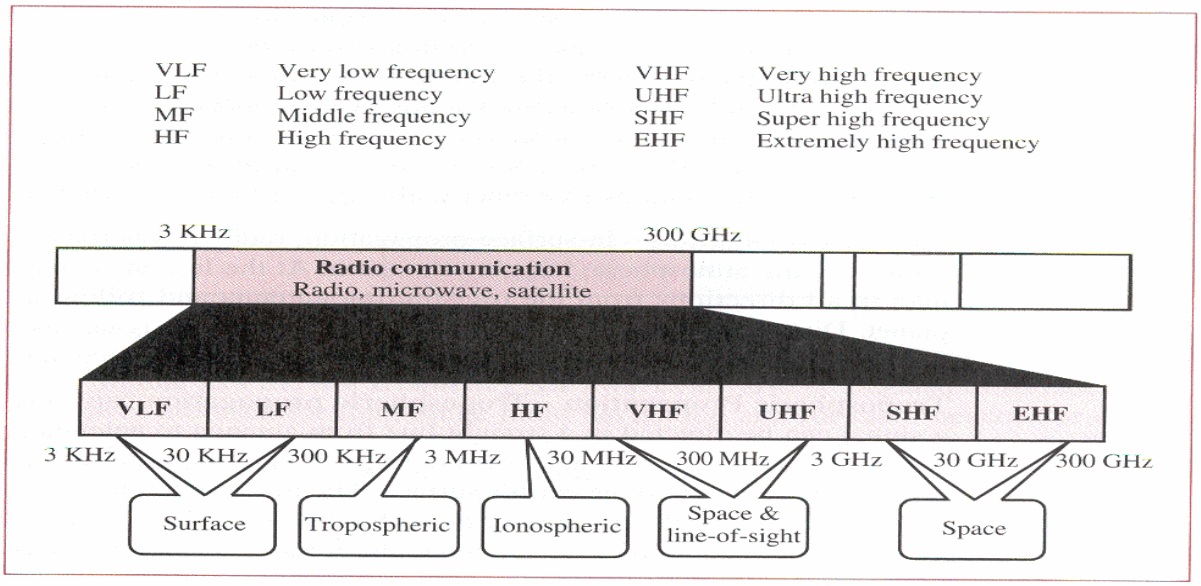
Fiber optics cable:

- Metal cables transmit signals in the form of electric current.
- Optical fiber is made of glass or plastic and transmits signals in the form of light.
- Light, a form of electromagnetic energy, travels at 300,000 Kilometers/second (186,000 miles/second), in a vacuum.
- The speed of the light depends on the density of the medium through which it is traveling (the higher density, the slower the speed).



Unguided media is also called wireless where not any physical path is used for transmission. Examples of unguided media are:- Microwave or Radio Links, Infrared.

Figure 7.21 *Radio communication band*



Band	Range	Propagation	Application
VLF	3–30 KHz	Ground	Long-range radio navigation
LF	30–300 KHz	Ground	Radio beacons and navigational locators
MF	300 KHz–3 MHz	Sky	AM radio
HF	3–30 MHz	Sky	Citizens band (CB), ship/aircraft communication
VHF	30–300 MHz	Sky and line-of-sight	VHF TV, FM radio
UHF	300 MHz–3 GHz	Line-of-sight	UHF TV, cellular phones, paging, satellite
SHF	3–30 GHz	Line-of-sight	Satellite communication
EHF	30–300 GHz	Line-of-sight	Long-range radio navigation

Transmission impairments:

1. Attenuation
2. Distortion
3. Noise

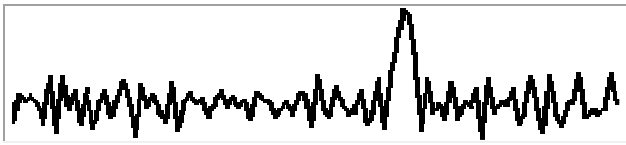
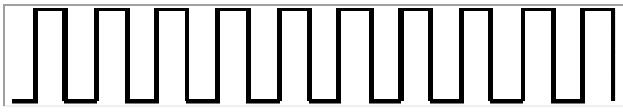
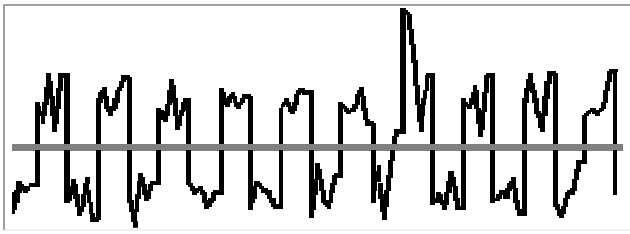
Attenuation: In computer networking, attenuation is a loss of signal strength measured in decibels (dB). Attenuation occurs on networks for several reasons:

- Range - both wireless and wired transmissions gradually dissipate in strength over longer reaches
- Interference - on wireless networks, radio interference or physical obstructions like walls also dampen communication signals
- Wire size - on wired networks, thinner wires suffer from higher (more) attenuation than thicker wires.

Distortion:

- Various frequency components making up the signal arrive at the receiver with varying delays.
- Inter symbol Interference - the frequency components are delayed and they start to interfere With the frequency components associated with the later bit.
- Only in guided media.
- Propagation velocity varies with frequency.

Noise:

Noise	
Signal	
signal + noise	

	Signals are reconstructed by sampling. Increased data rate implies "shorter" bits with higher sensitivity to noise.

Sources:
Thermal Agitates the electrons in conductors, and is a function of the temperature. It is often referred to as white noise, because it affects uniformly the different frequencies.

- The thermal noise in a bandwidth W is
  $N = kTW$
  where T=temperature, and k= Boltzmann's constant = 1.38 .10^{-23} Joules/degrees Kelvin.
- Signal to noise ratio: $(S/N)_{dB} = 10 \log \frac{\text{signal power}}{\text{noise power}}$ Typically measured at the receiver, because it is the point where the noise is to be removed from the signal.

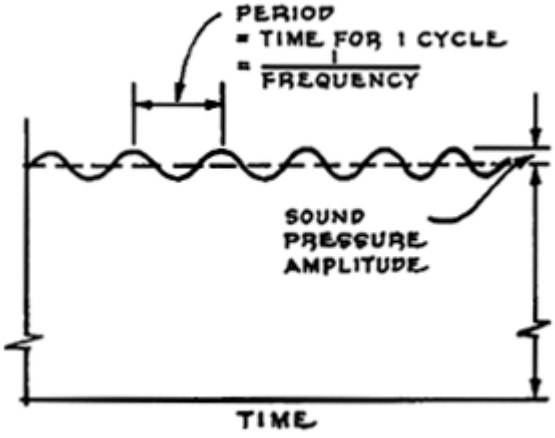
Inter modulation Resulting from interference of different frequencies sharing the same medium. It is caused by a component malfunction or a signal with excessive strength is used.
For example, the mixing of signals at frequencies f_1 and f_2 might produce energy at the frequency $f_1 + f_2$. This derived signal could interfere with an intended signal at frequency $f_1 + f_2$.
Crosstalk Foreign signal enters the path of the transmitted signal.
Impulse Irregular disturbances, such as lightning, and flawed communication elements. It is a primary source of error in digital data.

Throughput:
Throughput refers to how much data can be transferred from one place to another in a given amount of time. This can be calculated in bits per second.

For example, a hard drive that has a maximum transfer rate of 100 Mbps has twice the throughput of a drive that can only transfer data at 50 Mbps. Similarly, a 54 Mbps wireless connection has roughly 5 times as much throughput as a 11 Mbps connection. However, the actual data transfer speed may be limited by other factors such as the Internet connection speed and other network traffic.

Propagation speed and time, wavelength:

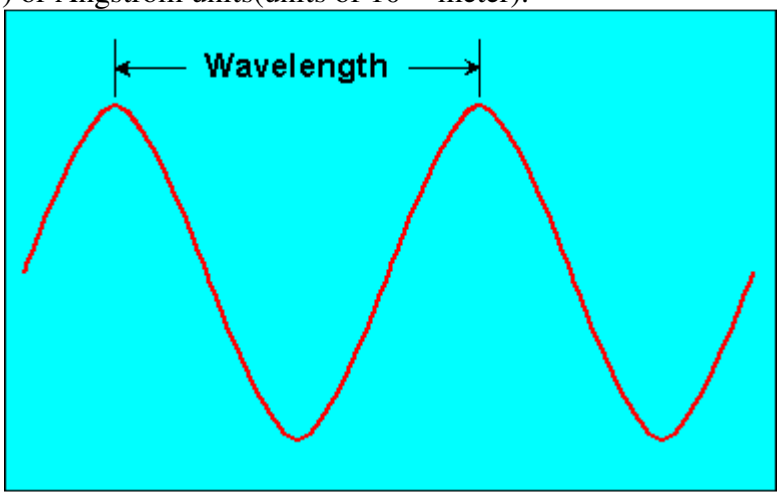
Propagation is defined as the movement of waves across the medium defined within the limits for the nature of wave. The propagation speed varies accordingly depending upon the various characteristics of the medium and waves. For instance, the electromagnetic wave, the mechanism of propagation involves mutual generation of periodically varying electric and magnetic fields and is far more difficult to understand than sound.



Wave Propagation Speed of a transmission medium is the speed at which a wave front passes through the medium, relative to the speed of light. For optical signals, the velocity factor is the reciprocal of the refractive index.

Time T of a wave is the time that elapses between the arrival of two consecutive crests (or troughs) at a certain location X. This definition is identical with the statement that the period is the time the vibration at X takes to complete a full cycle from crest to trough to crest. The period of a wave is given in seconds.

Wavelength λ, is the distance between identical points in the adjacent cycles of a waveform signal propagated in space or along a wire, as shown in the illustration. In wireless systems, this length is usually specified in meters, centimeters, or millimeters. In the case of infrared, visible light, ultraviolet, and gamma radiation, the wavelength is more often specified in nanometers (units of 10^{-9}meter) or Angstrom units(units of 10^{-10} meter).



Wavelength is inversely related to frequency. The higher the frequency of the signal, the shorter the wavelength. If *f* is the frequency of the signal as measured in megahertz, and *w* is the wavelength as measured in meters, then

$$w = 300/f$$

and conversely

$$f = 300/w$$

Wavelength is sometimes represented by the Greek letter lambda.

Shannon Capacity:

It is used to calculate the signal to noise ratio. The formula is:

$$C = B \log_2 \left(1 - \frac{S}{N}\right)$$

C is measured in bits per second if the logarithm is taken in base 2, or n at s per second if the natural logarithm is used, assuming *B* is in hertz; the signal and noise powers *S* and *N* are measured in watts or volts^2, so the signal-to-noise ratio here is expressed as a power ratio, *not* in decibels (dB); since figures are often cited in dB, a conversion may be needed. For example, 30 dB is a power ratio of $10^{30/10} = 10^3 = 1000$.

Example: Consider a noiseless channel with a bandwidth of 3000 Hz transmitting a signal with two signal levels. The maximum bit rate can be calculated as:

Bit rate=2*3000*$\log_2$ 2=6000bps

Unit – II

Telephony: Multiplexing: Many to one, one to many

Multiplexing is sending multiple signals from a single link. It means n number of inputs and single output. Multiplexing is sending multiple signals or streams of information on a carrier at the same time in the form of a single, complex signal and then recovering the separate signals at the receiving end.

There are basically three types of multiplexing is used.

1. WDM(wave division multiplexing)
2. TDM (Time division multiplexing)
3. FDM (Frequency division multiplexing)

Wavelength Division Multiplexing (WDM):

•In optical transmissions, FDM is known as Wavelength Division Multiplexing (WDM).
•With light different frequencies correspond to different colors.
•Several transmissions can be sending over the same fiber by using different light colors, and combining into a single light stream.
•Prisms are used as multiplexors and demultiplexors.

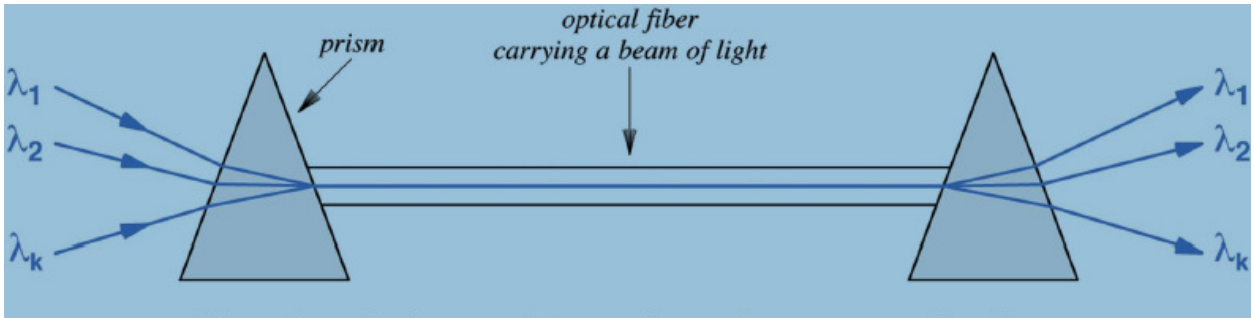


Illustration of prisms used to combine and separate wavelengths of light in wavelength division multiplexing technologies.

Time Division Multiplexing (TDM):
•It means dividing the available transmission time into time slots, and allocating a different slot to each transmitter.
•One method for transmitters to take turns is to transmit in round-robin order.

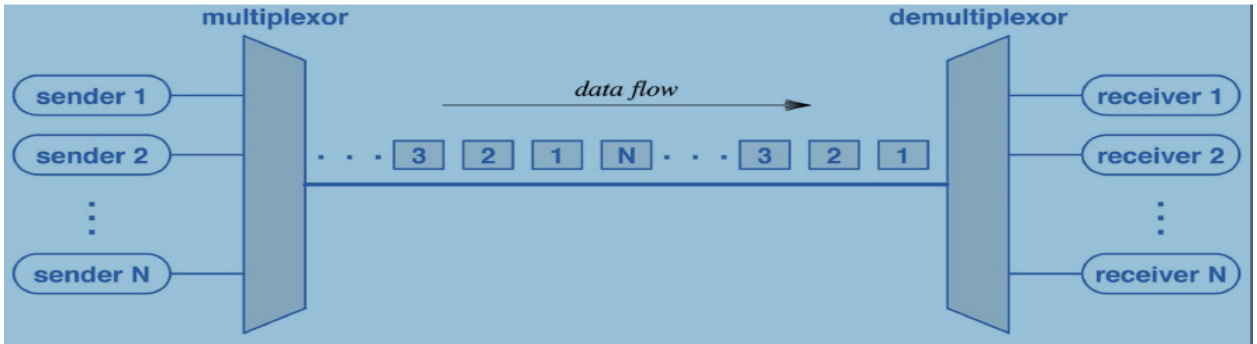


Illustration of the Time Division Multiplexing (TDM) concept with items from multiple sources sent over a shared medium.

Frequency Division Multiplexing (FDM):
•It is the basis for broadcast radio.
•Several stations can transmit simultaneously without interfering with each other provided they use separate carrier frequencies (separate channels).
•In data communications FDM is implemented by sending multiple carrier waves over the same copper wire.
•At the receiver's end, demultiplexing is performed by filtering out the frequencies other than the one carrying the expected transmission.
•Any of the modulation methods discussed before can be used to carry bits within a channel.

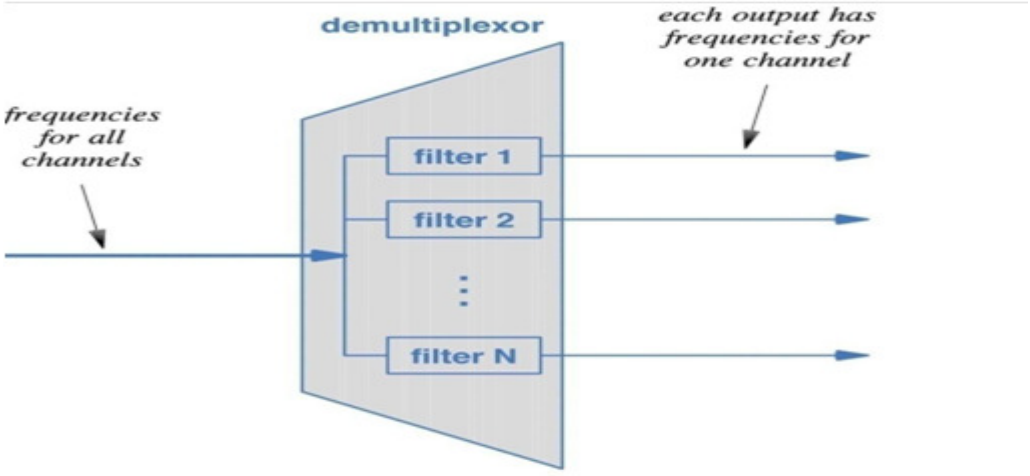


Illustration of the basic FDM demultiplexing where a set of filters each selects the frequencies for one channel and suppresses other frequencies.

Error control:

Error detection and correction:

Error:
• Frame = m data bits + r bits for error control. – n = m + r.
• Given the original frame f and the received frame f', how many corresponding bits differ?
– Hamming distance (Hamming, 1950).

Parity Bit:
• Simple error detecting code.
• Even- or odd parity.
• Example:
– Transmit 1011010.
– Add parity bit 1011010 0 (even parity) or 1011010 1 (odd parity).

Hamming Code:
• Check bits in power-of-two positions.
• Each check bit verifies a set of data bits.
• A data bit is checked by multiple check bits.
• Bits in positions that are power of 2 are check bits. The rest are data bits.
• Each check bit used in parity (even or odd) computation of collection of bits.
– Example: check bit in position 11, checks for bits in positions, 11 = 1+2+8. Similarly, bit 11 is checked by bits 1, 2, and 8.

• Parity computations:
– 11: 1, 2, 8 - 6: 2, 4
– 10: 2, 8 - 5: 1, 4
– 9: 1, 8 - 3: 1, 2
– 7: 1, 2, 4

Hamming Code: Example 1
11 10 9 8 7 6 5 4 3 2 1
1: 1, 3, 5, 7, 9, 11
Data: 1001101 using even parity (counting from right to left).
11 10 9 8 7 6 5 4 3 2 1
2: 3, 6, 7, 10, 11
1 0 0 1 1 0 1 1
1 0 0 1 1 1 0 0 1 0 1

Hamming Code: Example 2
What if instead of 1 0 0 1 1 1 0 0 10 1, receiver gets 1 0 0 1 0 1 0 0 1 0 1?
Receiver takes frame received and re-computes check bits.
1: 3, 5, 7, 9, 11: 1, 1, 0, 1, 0, 1 => 1
2: 3, 6, 7, 10, 11: 0, 1, 1, 0, 0, 1 => 1
4: 5, 6, 7 : 0, 0, 1, 0 => 1
8: 9, 10, 11: 1, 0, 0, 1 => 0
11 10 9 8 7 6 5 4 3 2 1
0 1 1 1
Result: Bit in position 0 1 1 1 is wrong!

How much code redundancy?
• How many check bits needed, i.e., given m data bits, how many more bits (r) are needed to allow all single-bit errors to be corrected?
– Resulting frame is m + r.
– (m+r+1) <= 2r.
– Given m, then find r.
– Example: If m = 7 (ASCII 7 code), minimum r is 4.

Hamming Code: Example 7-bit
. Hamming codes can only correct single errors.
. But, to correct bursts of errors, send column by column.

Error Detecting Codes
• Typically used in reliable media.
• Examples: parity bit, polynomial codes (CRC, or Cyclic redundancy Check).

Polynomial Codes
• Treat bit strings as representations of polynomials with coefficients 1's and 0's.
• K-bit frame is coefficient list of polynomial with k terms (and degree k-1), from xk-1to x0.
– Highest-order bit is coefficient of xk-1, etc.
– Example: 110001 represent x5 + x4 +x0.
• Generator polynomial G(x).
– Agreed upon by sender and receiver.

CRC:
• Checksum appended to frame being transmitted.
– Resulting polynomial divisible by G(x).
• When receiver gets checksum frame, it divides it by G(x).
– If remainder, then error!

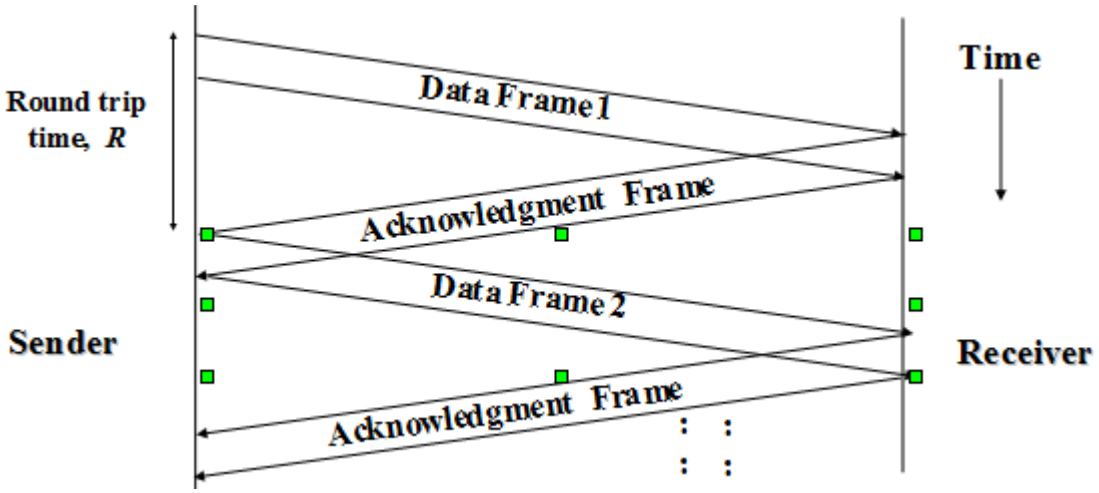
Cyclic Redundancy Check
At Transmitter, with M = 1 1 1 0 1 1, compute 2rM= 1 1 1 0 1 1 0 0 0 with G = 1 1 0 1
T = 2rM + R [note G starts and ends with "1" R = 1 1 1 Transmit T= 1 1 1 0 1 1 1 1 1

Cyclic Redundancy Check
At the Receiver, compute:
Note remainder = 0 no errors detected

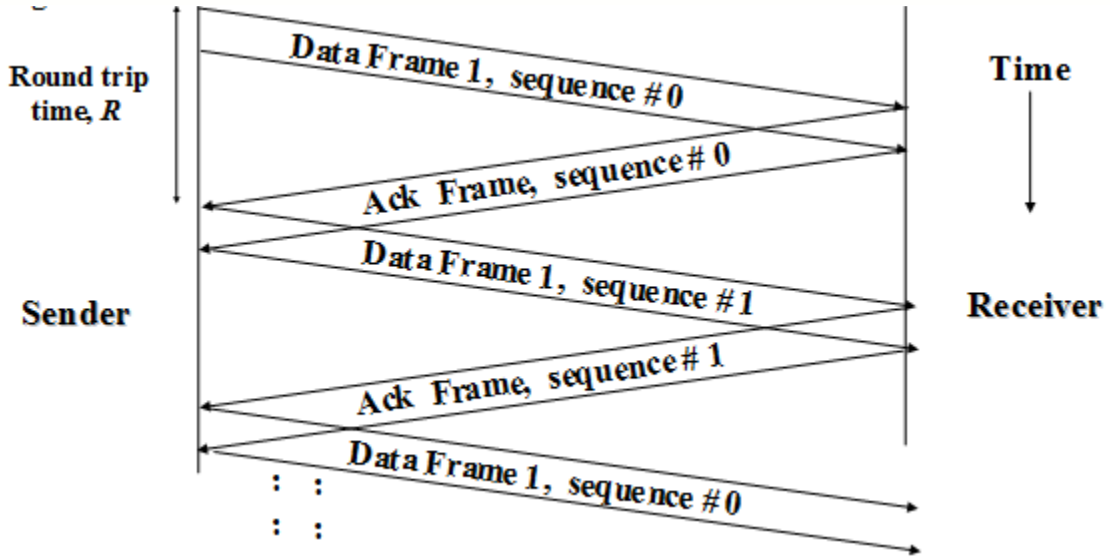
CRC Performance
• Errors go through undetected only if divisible by G(x)
• With "suitably chosen" G(x) CRC code detects all single-bit errors.

Flow and error control: Different techniques to control the overflow of data and different errors in transmission are called as Flow and error control techniques. Some techniques are as Follows:

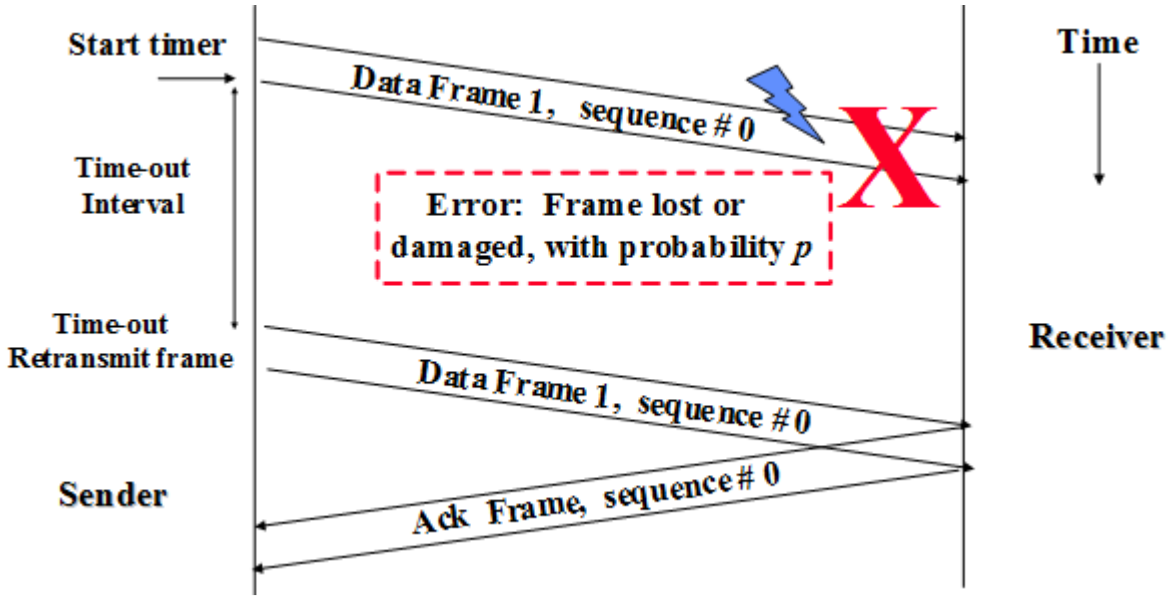
Simplex Stop-and-Wait Protocol:
Simplex: Data transmission in one direction. The receiver may not be always ready to receive the next frame (finite buffer storage). Receiver sends a positive acknowledgment frame to sender to transmit the next data frame. Error-free communication channel assumed. No retransmissions used.



A Simplex Positive Acknowledgment with Retransmission (PAR) Protocol. The receiver may not be always ready to receive the next frame (finite buffer storage). Noisy communication channel; frames may be damaged or lost. Frame not received correctly with probability P Receiver sends a positive acknowledgment frame to sender to transmit the next data frame. Any frame has a sequence number, either 0 or 1 Maximum utilization and throughput similar to protocol 2 when the effects of errors are ignored.



A Simplex PAR Protocol (continued) Effect of Errors The sender starts a timer when transmitting a data frame. If data frame is lost or damaged (probability = p): Receiver does not send an acknowledgment Sender times out and retransmits the data frame



Flow Control Sliding Window Protocols:

These protocols allow both link nodes (A, B) to send and receive data and acknowledgments simultaneously. Acknowledgments are piggybacked into an acknowledgment field in the data frame header not as separate frames. If no new data frames are ready for transmission in a specified time, a separate acknowledgment frame is generated to avoid time-out. Each outbound frame contains a sequence number ranging from 0 to 2 n-1 (n-bit field). N = 1 for stop-and-wait sliding window protocols.

Sending window: A set of sequence numbers maintained by the sender and correspond to frame sequence numbers of frames sent out but not acknowledged. The maximum allowed size of the sending window w correspond to the maximum number of frames the sender can transmit before receiving any acknowledgment without blocking (pipelining). All frames in the sending window may be lost or

damaged and thus must be kept in memory or buffers until they are acknowledged. Sliding Window Data Link Protocols

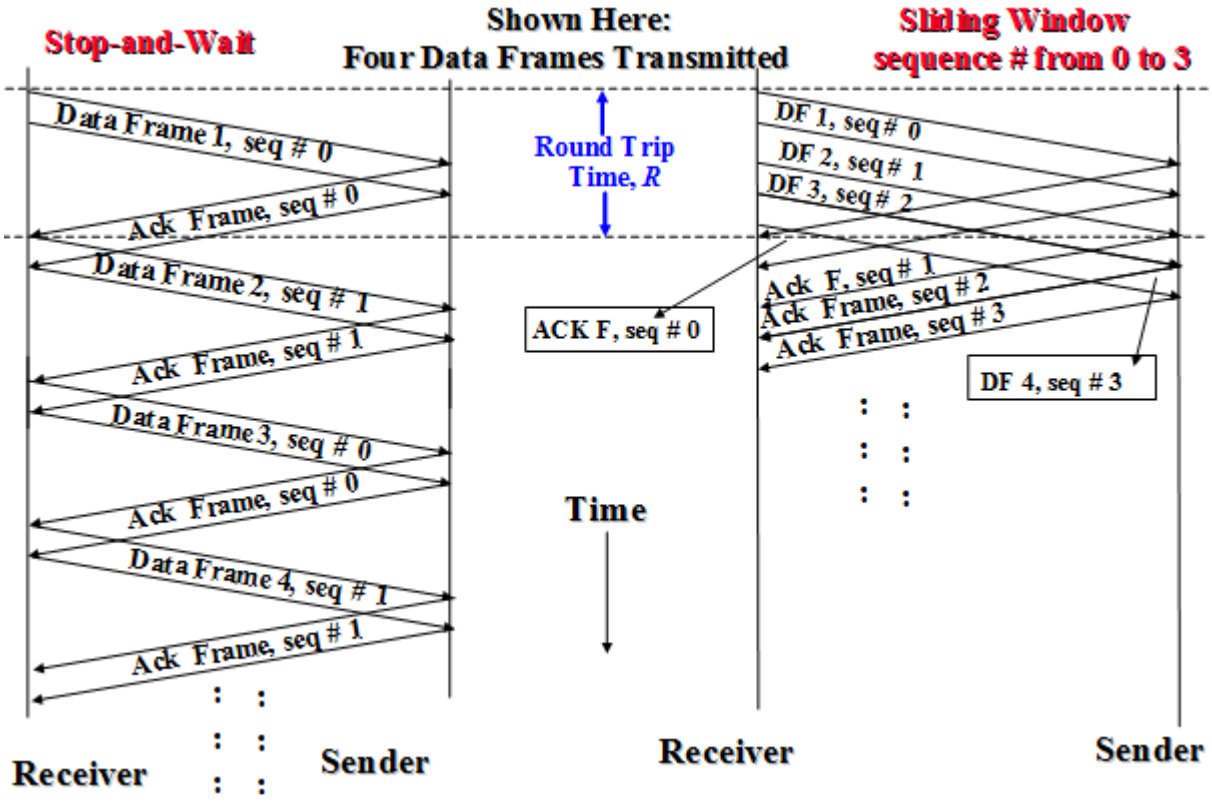
Receiving window: A set of sequence numbers maintained by the receiver and indicate the frames sequence numbers it is allowed to receive and acknowledge. The size of the receiving window is fixed at a specified initial size. Any frame received with a sequence number outside the receiving window is discarded. The sending window and receiving window may not have the same upper or lower limits or have the same size. When pipelining is used, an error in a frame is dealt with in one of two ways:

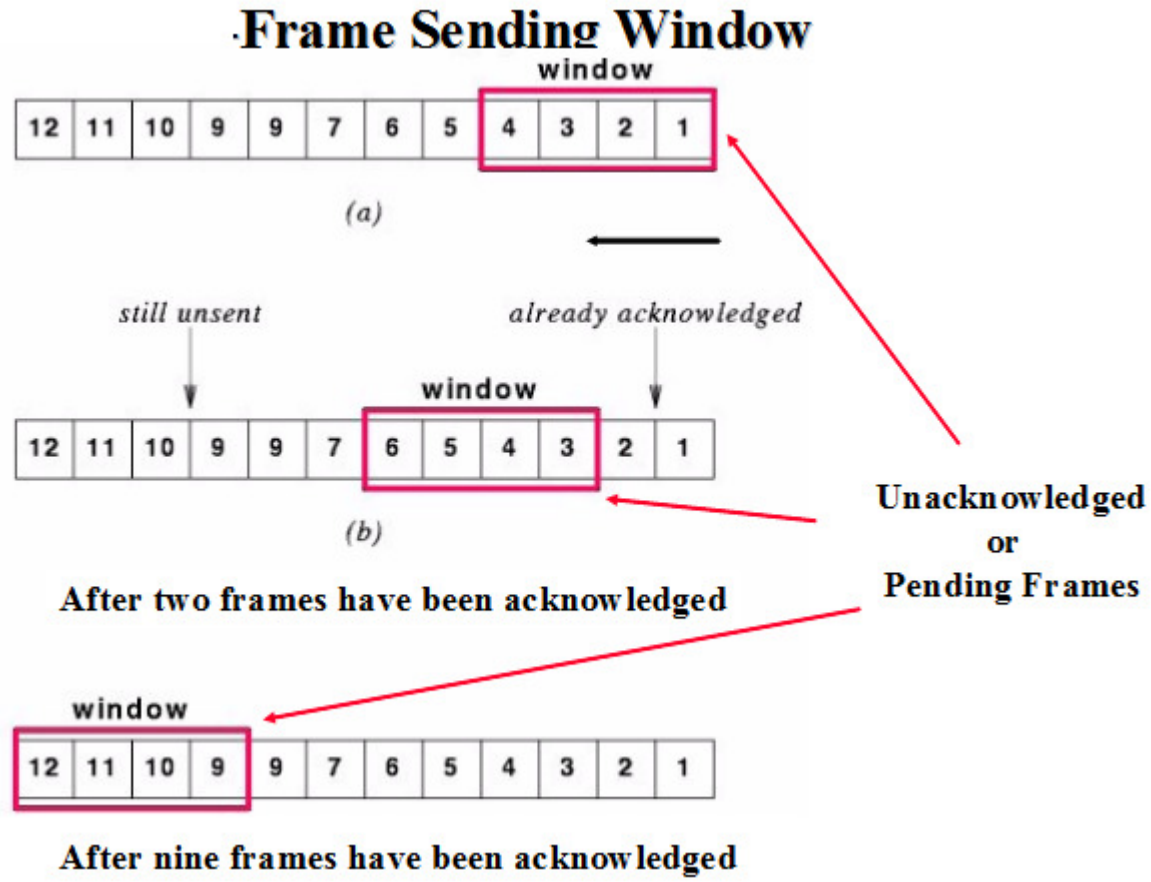
Go back n:

The receiver discards all subsequent frames and sends no acknowledgments. The sender times out and resends all the discarded frames starting with faulty frame.

Selective repeat:

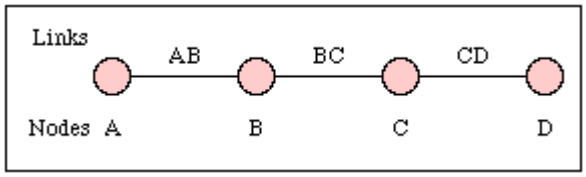
The receiving data link stores all good frames received after a bad frame. Only the bad frame is retransmitted upon time-out by the sender.





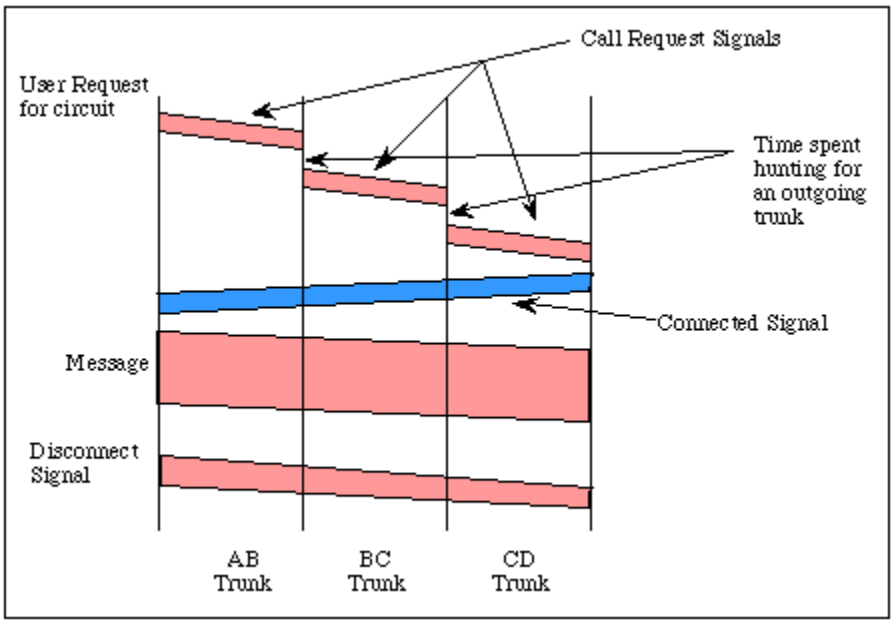
Circuit switching:

Circuit switching is the most familiar technique used to build a communications network. It is used for ordinary telephone calls. It allows communications equipment and circuits, to be shared among users. Each user has sole access to a circuit (functionally equivalent to a pair of copper wires) during network use. Consider communication between two points A and D in a network. The connection between A and D is provided using (shared) links between two other pieces of equipment, B and C.



A connection between two systems A & D formed from 3 links

Network use is initiated by a connection phase, during which a circuit is set up between source and destination, and terminated by a disconnect phase. These phases, with associated timings, are illustrated in the figure below.



A circuit switched connection between A and D

(Information flows in two directions. Information sent from the calling end is shown in pink and information returned from the remote end is shown in blue)

After a user requests a circuit, the desired destination address must be communicated to the local switching node (B). In a telephony network, this is achieved by dialing the number.

Node B receives the connection request and identifies a path to the destination (D) via an intermediate node (C). This is followed by a circuit connection phase handled by the switching nodes and initiated by allocating a free circuit to C (link BC), followed by transmission of a call request signal from node B to node C. In turn, node C allocates a link (CD) and the request is then passed to node D after a similar delay.

The circuit is then established and may be used. While it is available for use, resources (i.e. in the intermediate equipment at B and C) and capacity on the links between the equipment are dedicated to the use of the circuit.

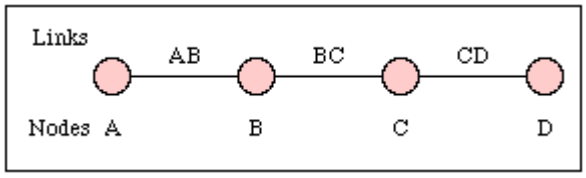
After completion of the connection, a signal confirming circuit establishment (a connect signal in the diagram) is returned; this flows directly back to node A with no search delays since the circuit has been established. Transfer of the data in the message then begins. After data transfer, the circuit is disconnected; a simple disconnect phase is included after the end of the data transmission.

Delays for setting up a circuit connection can be high, especially if ordinary telephone equipment is used. Call setup time with conventional equipment is typically on the order of 5 to 25 seconds after completion of dialing. New fast circuit switching techniques can reduce delays. Trade-offs between circuit switching and other types of switching depend strongly on switching times.

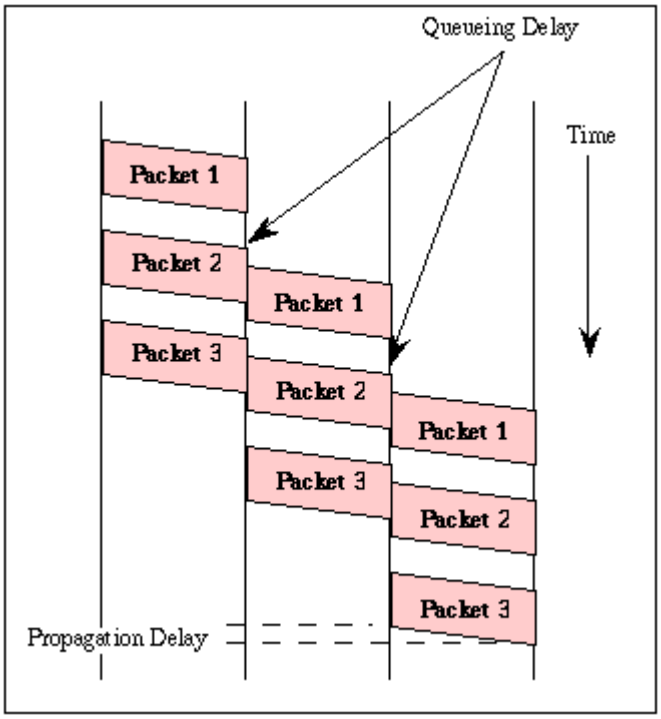
Packet switching:

Packet switching is similar to message switching using short messages. Any message exceeding a network-defined maximum length is broken up into shorter units, known as packets, for transmission; the packets, each with an associated header, are then transmitted individually through the network. The fundamental difference in packet communication is that the data is formed into packets with a pre-defined header format (i.e. PCI), and well-known "idle" patterns which are used to occupy the link when there is no data to be communicated.

Packet network equipment discards the "idle" patterns between packets and processes the entire packet as one piece of data. The equipment examines the packet header information (PCI) and then either removes the header (in an end system) or forwards the packet to another system. If the out-going link is not available, then the packet is placed in a queue until the link becomes free. A packet network is formed by links which connect packet network equipment.



Communication between A and D using circuits which are shared using packet switching.



Packet-switched communication between systems A and D

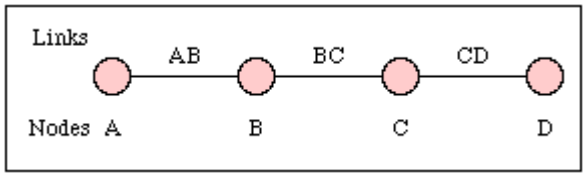
(The message in this case has been broken into three parts labeled 1-3)

There are two important benefits from packet switching.

1. The first and most important benefit is that since packets are short, the communication links between the nodes are only allocated to transferring a single message for a short period of time while transmitting each packet. Longer messages require a series of packets to be sent, but do not require the link to be dedicated between the transmission of each packet. The implication is that packets belonging to other messages may be sent between the packets of the message being sent from A to D. This provides a much fairer sharing of the resources of each of the links.
2. Another benefit of packet switching is known as "pipelining". Pipelining is visible in the figure above. At the time packet 1 is sent from B to C, packet 2 is sent from A to B; packet 1 is sent from C to D while packet 2 is sent from B to C, and packet 3 is sent from A to B, and so forth. This simultaneous use of communications links represents a gain in efficiency; the total delay for transmission across a packet network may be considerably less than for message switching, despite the inclusion of a header in each packet rather than in each message.

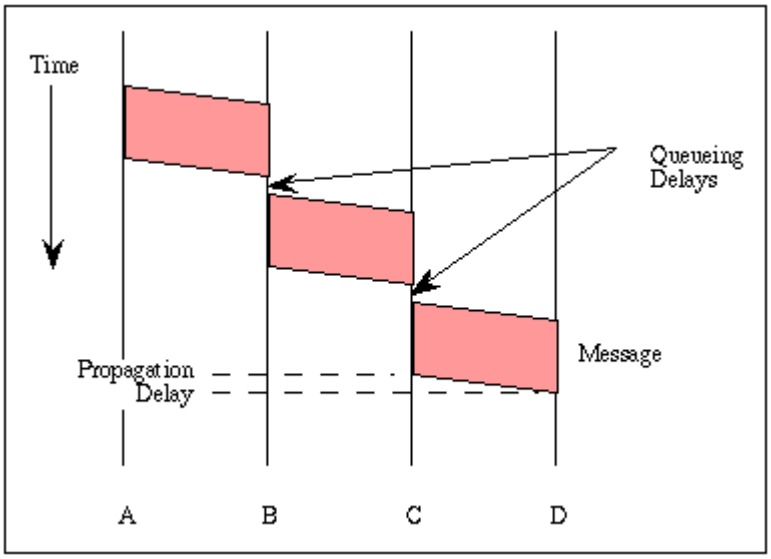
Message switching:

Sometimes there is no need for a circuit to be established all the way from the source to the destination. Consider a connection between the users (A and D) in the figure below (i.e. A and D) is represented by a series of links (AB, BC, and CD).



A connection between two systems A & D formed from 3 links

For instance, when a telex (or email) message is sent from A to D, it first passes over a local connection (AB). It is then passed at some later time to C (via link BC), and from there to the destination (via link CD). At each message switch, the received message is stored, and a connection is subsequently made to deliver the message to the neighboring message switch. Message switching is also known as store-and-forward switching since the messages are stored at intermediate nodes en route to their destinations.

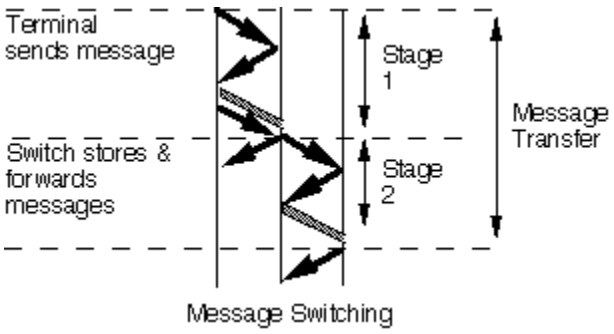


The use of message switching to communicate between A and D

The figure illustrates message switching; transmission of only one message is illustrated for simplicity. As the figure indicates, a complete message is sent from node A to node B when the link interconnecting them becomes available. Since the message may be competing with other messages for access to facilities, a queuing delay may be incurred while waiting for the link to become available. The message is stored at B until the next link becomes available, with another queuing delay before it can be forwarded. It repeats this process until it reaches its destination.

Circuit setup delays are replaced by queuing delays. Considerable extra delay may result from storage at individual nodes. A delay for putting the message on the communications link (message length in bits divided by link speed in bps) is also incurred at each node en route. Message lengths are slightly longer than they are in circuit switching, after establishment of the circuit, since header information must be included with each message; the header includes information identifying the destination as well as other types of information.

Most message switched networks do not use dedicated point-to-point links and therefore a call must be set-up using a circuit switched network. The figure below illustrates the use of message switching over a circuit switched network, in this case using one intermediate message switch.



Message switching using circuit switched connections between message switches.

Although message switching is still used for electronic mail and telex transmission, it has largely been replaced by packet switching (in fact, most electronic mail is carried using message switching with the links between message switches provided by packet or circuit-switched networks).

Data Link control protocols:

Line discipline

Various synchronous protocols manage communications on computer motherboards.

The terms "synchronous" and "asynchronous" refer to the two different styles of exchanging information in a digital system between two ports or devices. In both styles, messages need to be organized in order to ensure that they are properly handled. Synchronous messages typically use some sort of external clock to match data exchange, while asynchronous messages simply move at their own individual rates of speed, relying on established systems of rules to ensure proper routing. All computer systems employ both methods of communication and there are a number of different protocols for each

synchronous and asynchronous protocols overview:

File Transfer Protocols

- File transfer protocols are examples of asynchronous communication protocols. File Transfer Protocol (FTP), Apple Filing Protocol (AFP) and Bit Torrent are all examples of file transfer protocols. Typically, they divide data into small packets of bits, which are then sent over a network to a destination one at a time. A packet is not sent until the sender receives confirmation from the recipient that the previous packet has been received.

Email

- There are three major protocols for sending and receiving email messages. Simple Mail Transfer Protocol (SMTP) is an asynchronous protocol most often used to send email. Post Office Protocol (POP) and Internet Message Access Protocol (IMAP) are both asynchronous protocols most often used for receiving email.

World Wide Web

- The World Wide Web is entirely made up of asynchronous protocols. The most common is Hypertext Transfer Protocol (HTTP), though web sites also use Hypertext Transfer Protocol Secure (HTTPS) among other protocols for exchanging information over the web.

Serial Peripheral Interface Bus

- The Serial Peripheral Interface Bus (SPI) is a synchronous communication protocol used to link computers within a formal system. Typically, computers are linked into a master-slave relationship where one computer is the "master" controlling the other "slaves."

Inter-Integrated Circuit

- Inter-Integrated Circuit (I2C) is a synchronous protocol for connecting devices such as drives, input/output devices and printers to a motherboard or other computer control system. I2C is a

very common method for linking peripheral devices to computers, and has become the basis for a number of other technological systems such as the System Management Bus (SMB) that controls power to computer motherboards.

ISDN:

Integrated Services Digital Network (ISDN) is a set of communication standards for digital transmission of voice, video, data, and other network services over the traditional circuits of the public switched telephone network.

Historical outline:

It was first defined in 1988 in the CCITT red book. 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. There are several kinds of access interfaces to ISDN defined as Basic Rate Interface (BRI), Primary Rate Interface (PRI), Narrowband ISDN (N-ISDN), and Broadband ISDN (B-ISDN).

Subscriber's access:

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. A major market application for ISDN in some countries is Internet access, where ISDN typically provides a maximum of 128 kbps 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 kbps channels) are bonded.

ISDN Layers:

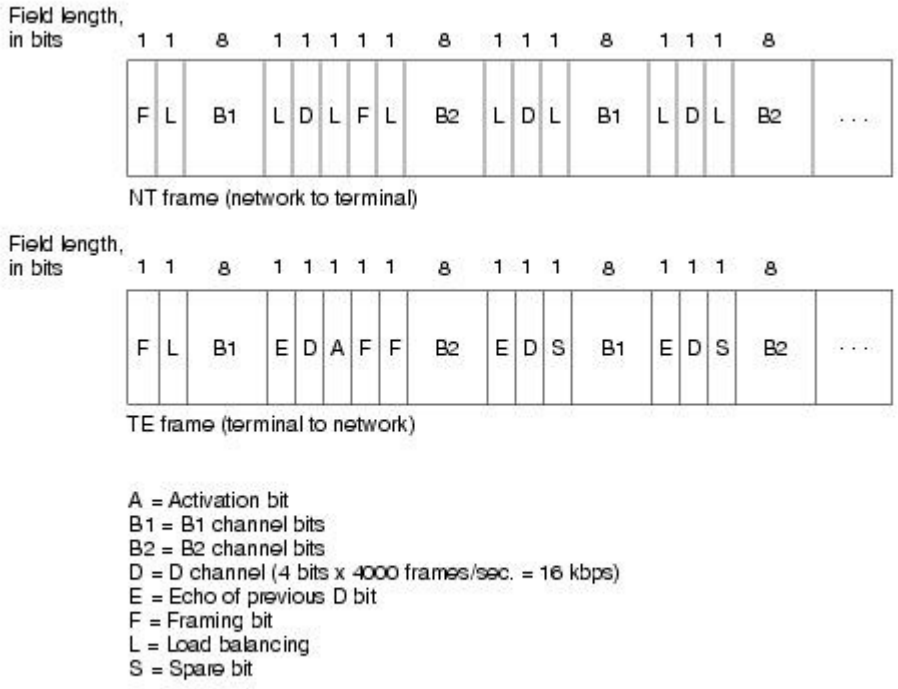
Layer 1

ISDN physical layer (Layer 1) frame formats differ depending on whether the frame is outbound (from terminal to network) or inbound (from network to terminal).

In the figure frames are 48 bits long, of which 36 bits represent data. The bits of an ISDN physical layer frame are used as follows:

- F - Provides synchronization
- L - Adjusts the average bit value
- E - Ensures contention resolution when several terminals on a passive bus contend for a channel
- A - Activates devices
- S - Is unassigned
- B1, B2, and D - Handle user data

Figure: ISDN Physical Layer Frame Formats Differ Depending on Their Direction



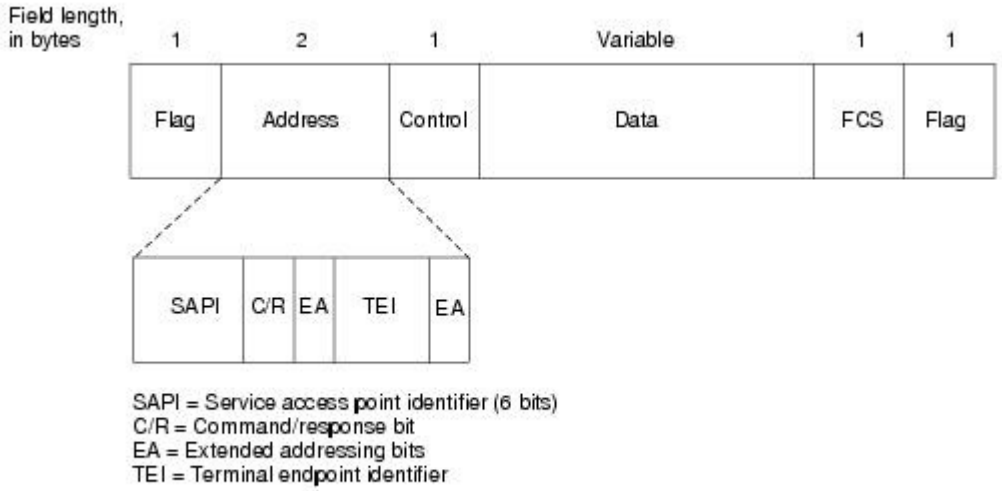
Multiple ISDN user devices can be physically attached to one circuit. In this configuration, collisions can result if two terminals transmit simultaneously. Therefore, ISDN provides features to determine link contention. When an NT receives a D bit from the TE, it echoes back the bit in the next E-bit position. The TE expects the next E bit to be the same as its last transmitted D bit.

Terminals cannot transmit into the D channel unless they first detect a specific number of one's (indicating "no signal") corresponding to a pre-established priority. If the TE detects a bit in the echo (E) channel that is different from its D bits, it must stop transmitting immediately. This simple technique ensures that only one terminal can transmit its D message at one time. After successful D-message transmission, the terminal has its priority reduced by requiring it to detect more continuous ones before transmitting. Terminals cannot raise their priority until all other devices on the same line have had an opportunity to send a D message. Telephone connections have higher priority than all other services, and signaling information has a higher priority than non signaling information.

Layer 2

Layer 2 of the ISDN signaling protocol is Link Access Procedure, D channel (LAPD). LAPD is similar to High-Level Data Link Control (HDLC) and Link Access Procedure, Balanced (LAPB). As the expansion of the LAPD acronym indicates, this layer is used across the D channel to ensure that control and signaling information flows and is received properly.

Figure: LAPD Frame Format Is Similar to That of HDLC and LAPB

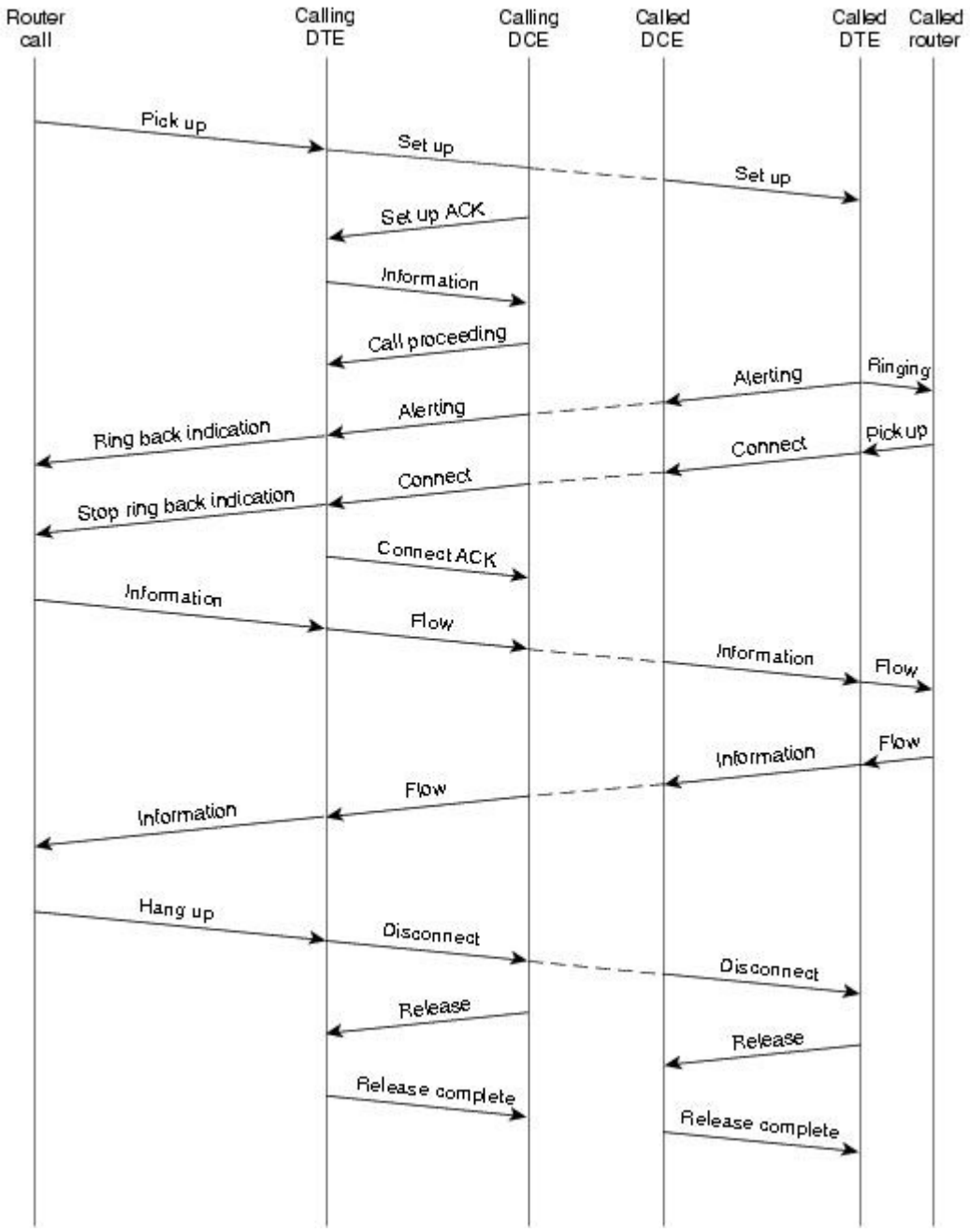


The LAPD Flag and Control fields are identical to those of HDLC. The LAPD Address field can be either 1 or 2 bytes long. If the extended address bit of the first byte is set, the address is 1 byte; if it is not set, the address is 2 bytes. The first Address-field byte contains the service access point identifier (SAPI), which identifies the portal at which LAPD services are provided to Layer 3. The C/R bit indicates whether the frame contains a command or a response. The Terminal Endpoint Identifier (TEI) field identifies either a single terminal or multiple terminals. A TEI of all ones indicates a broadcast.

Layer 3

Two Layer 3 specifications are used for ISDN signaling: ITU-T (formerly CCITT) I.450 (also known as ITU-T Q.930) and ITU-T I.451 (also known as ITU-T Q.931). Together, these protocols support user-to-user, circuit-switched, and packet-switched connections. A variety of call-establishment, call-termination, information, and miscellaneous messages are specified, including SETUP, CONNECT, RELEASE, USER INFORMATION, CANCEL, STATUS, and DISCONNECT. These messages are functionally similar to those provided by the X.25 protocol.

Figure: An ISDN Circuit-Switched Call Moves through Various Stages to Its Destination



Broadband ISDN: Broadband Integrated Services Digital Network (BISDN)

Broadband Integrated Services Digital Network (BISDN or Broadband ISDN) is designed to handle high-bandwidth applications. BISDN currently uses ATM technology over SONET-based transmission circuits

to provide data rates from 155 to 622Mbps and beyond, contrast with the traditional narrowband ISDN (or N-ISDN), which is only 64 Kbps basically and up to 2 Mbps.

The designed Broadband ISDN (BISDN) services can be categorized as follows:

- Conversational services such as telephone-like services, which was also supported by N-ISDN. Also the additional bandwidth offered will allow such services as video telephony, video conferencing and high volume, high speed data transfer.
- Messaging services, which is mainly a store-and-forward type of service. Applications could include voice and video mail, as well as multi-media mail and traditional electronic mail.
- Retrieval services which provides access to (public) information stores, and information is sent to the user on demand only.
- No user control of presentation. This would be for instance, a TV broadcast, where the user can choose simply either to view or not.
- User controlled presentation. This would apply to broadcast information that the user can partially control.

Unit-III

Network Devices: Repeaters, bridges, gateways, routers:

Repeater: A **repeater** is an electronic device that receives a signal and retransmits it at a higher level or higher power, or onto the other side of an obstruction, so that the signal can cover longer distances without degradation. In most twisted pair Ethernet configurations, repeaters are required for cable runs longer than 100 meters.

Bridges: A **network bridge** connects multiple network segments at the data link layer of the OSI model. Bridges do not promiscuously copy traffic to all ports, as a hub do, but learns which MAC addresses are reachable through specific ports. Once the bridge associates a port and an address, it will send traffic for that address only to that port. Bridges do send broadcasts to all ports except the one on which the broadcast was received. Bridges learn the association of ports and addresses by examining the source address of frames that it sees on various ports. Once a frame arrives through a port, its source address is stored and the bridge assumes that MAC address is associated with that port. The first time that a previously unknown destination address is seen, the bridge will forward the frame to all ports other than the one on which the frame arrived.

Gateway: Gateways work on all seven OSI layers. The main job of a gateway is to convert protocols among communications networks. A router by itself transfers, accepts and relays packets only across networks using similar protocols. A gateway on the other hand can accept a packet formatted for one protocol (e.g. AppleTalk) and convert it to a packet formatted for another protocol (e.g. TCP/IP) before forwarding it. A gateway can be implemented in hardware, software or both, but they are usually implemented by software installed within a router. A gateway must understand the protocols used by each network linked into the router. Gateways are slower than bridges, switches and (non-gateway) routers. A gateway is a network point that acts as an entrance to another network. On the

Internet, a node or stopping point can be either a gateway node or a host (end-point) node. Both the computers of Internet users and the computers that serve pages to users are host nodes, while the nodes that connect the networks in between are gateways. For example, the computers that control traffic between company networks or the computers used by internet service providers (ISPs) to connect users to the internet are gateway nodes.

Router: A router is a key device in the internet communication and wan communication system. A router has software called routing table and the source and destination addresses are stored in the routing table. Routers are networking devices that forward data packets between networks using headers and forwarding tables to determine the best path to forward the packets. Routers work at the network layer of the TCP/IP model or layer 3 of the OSI model. Routers also provide interconnectivity between like and unlike media. This is accomplished by examining the Header of a data packet, and making a decision on the next hop to which it should be sent. They use preconfigured static routes, status of their hardware interfaces, and routing protocols to select the best route between any two subnets. A router is connected to at least two networks, commonly two LANs or WANs or a LAN and its ISP's network. Some DSL and cable modems, for home and office use, have been integrated with routers to allow multiple home/office computers to access the Internet through the same connection. Many of these new devices also consist of wireless access points (waps) or wireless routers to allow for IEEE 802.11b/g wireless enabled devices to connect to the network without the need for a cabled connection.

The Network Layer

Maintaining the quality of service requested by the transport layer.
The network layer performs network routing functions, and might also perform fragmentation and reassembly, and report delivery errors

Design Issues:

IPv4 Addresses:

Each device on a network must be uniquely defined. At the Network layer, the packets of the communication need to be identified with the source and destination addresses of the two end systems. With IPv4, this means that each packet has a 32-bit source address and a 32-bit destination address in the Layer 3 header. These addresses are used in the data network as binary patterns. Inside the devices, digital logic is applied for their interpretation. For us in the human network, a string of 32 bits is difficult to interpret and even more difficult to remember. Therefore, we represent IPv4 addresses using dotted decimal format.

Network Layer Addressing:

Dotted Decimal

Binary patterns representing IPv4 addresses are expressed as dotted decimals by separating each byte of the binary pattern, called an octet, with a dot. It is called an octet because each decimal number represents one byte or 8 bits.

For example, the address:
10101100000100000000010000010100
is expressed in dotted decimal as:
172.16.4.20
Keep in mind that devices use binary logic. The dotted decimal format is used to make it easier for people to use and remember addresses.

Class full Addressing

IP Address Classes

Address Class	1st octet range (decimal)	1st octet bits (green bits do not change)	Network(N) and Host(H) parts of address	Default subnet mask (decimal and binary)	Number of possible networks and hosts per network
A	1–127**	00000000–01111111	N.H.H.H	255.0.0.0	128 nets (2^7) 16,777,214 hosts per net (2^24–2)
B	128–191	10000000–10111111	N.N.H.H	255.255.0.0	16,384 nets (2^14) 65,534 hosts per net (2^16–2)
C	192–223	11000000–11011111	N.N.N.H	255.255.255.0	2,097,150 nets (2^21) 254 hosts per net (2^8–2)
D	224–239	11100000–11101111	NA (multicast)		
E	240–255	11110000–11111111	NA (experimental)		

** All zeros (0) and all ones (1) are invalid hosts addresses.

Routing concepts (Forwarding Function, Filtering Function):
Filtering: A filter is installed on the forwarding plane. This filter counts and applies the actions to the categories of traffic Because the filter is enforced in the forwarding plane, it prevents traffic from consuming bandwidth on the interface that connects the forwarding plane to the router control plane. The counters serve as an important forensic tool for the analysis of potential attacks, and as an invaluable debugging and troubleshooting aid. By adjusting the granularity and order of the filters, more granular forensics can be performed (i.e., create a filter that matches only traffic allowed from a group of IP addresses for a given protocol followed by a filter that denies all traffic for that protocol). This would allow for counters to be monitored for the allowed protocol filter, as well as any traffic matching the specific protocol that didn't originate from the explicitly allowed hosts.
Forwarding: In addition to the filters, rate limiters for certain classes of traffic are also installed in the forwarding plane. These rate limiters help further control the traffic that will reach the router control

plane for each filtered class as well as all traffic not matching an explicit class. The actual rates selected for various classes are network deployment specific; analysis of the rates required for stability should be done periodically. It is important to note that the most significant factor to consider regarding the traffic profile going to the router control plane is the packets per second (pps) rate. Therefore, careful consideration must be given to determine the maximum pps rate that could be generated from a given set of packet size and bandwidth usage scenarios.

Routing: is the act of moving information across an internetwork from a source to a destination. Along the way, at least one intermediate node typically is encountered.

Static Versus Dynamic:

Static routing algorithms are hardly algorithms at all, but are table mappings established by the network administrator before the beginning of routing. These mappings do not change unless the network administrator alters them. Algorithms that use static routes are simple to design and work well in environments where network traffic is relatively predictable and where network design is relatively simple.

Because static routing systems cannot react to network changes, they generally are considered unsuitable for today's large, constantly changing networks. Most of the dominant routing algorithms today are dynamic routing algorithms, which adjust to changing network circumstances by analyzing incoming routing update messages. If the message indicates that a network change has occurred, the routing software recalculates routes and sends out new routing update messages. These messages permeate the network, stimulating routers to rerun their algorithms and change their routing tables accordingly.

Dynamic routing algorithms can be supplemented with static routes where appropriate. A router of last resort (a router to which all unroutable packets are sent), for example, can be designated to act as a repository for all unroutable packets, ensuring that all messages are at least handled in some way

Hierarchical Routing :In a hierarchical routing system, some routers form what amounts to a routing backbone. Packets from nonbackbone routers travel to the backbone routers, where they are sent through the backbone until they reach the general area of the destination. At this point, they travel from the last backbone router through one or more nonbackbone routers to the final destination.

Routing systems often designate logical groups of nodes, called domains, autonomous systems, or areas. In hierarchical systems, some routers in a domain can communicate with routers in other domains, while others can communicate only with routers within their domain. In very large networks, additional hierarchical levels may exist, with routers at the highest hierarchical level forming the routing backbone.

The primary advantage of hierarchical routing is that it mimics the organization of most companies and therefore supports their traffic patterns well. Most network communication occurs within small company groups (domains). Because intradomain routers need to know only about other routers within their domain, their routing algorithms can be simplified, and, depending on the routing algorithm being used, routing update traffic can be reduced accordingly.

Distributed routing:

The key to a distributed routing is to apply a decomposition of problem. For solving the problem, we propose to apply the common approach of using any simple routing protocol.

Distance Vector Protocol, Link State protocol:

Link-state algorithms (also known as shortest path first algorithms) flood routing information to all nodes in the internetwork. Each router, however, sends only the portion of the routing table that describes the state of its own links. In link-state algorithms, each router builds a picture of the entire network in its routing tables. Distance vector algorithms (also known as Bellman-Ford algorithms) call for each router to send all or some portion of its routing table, but only to its neighbors. In essence, link-state algorithms send small updates everywhere, while distance vector algorithms send larger updates only to neighboring routers. Distance vector algorithms know only about their neighbors.

Because they converge more quickly, link-state algorithms are somewhat less prone to routing loops than distance vector algorithms. On the other hand, link-state algorithms require more CPU power and memory than distance vector algorithms. Link-state algorithms, therefore, can be more expensive to implement and support. Link-state protocols are generally more scalable than distance vector protocols.

Unit – IV

Transport layer:

In computer networking, the **transport layer** or **layer 4** provides end-to-end communication services for applications within a layered architecture of network components and protocols. The transport layer provides convenient services such as connection-oriented data stream support, reliability, flow control, and multiplexing.

Different protocols used in Transport layer

TCP
UDP
DCCP
SCTP
RSVP

The most well-known transport protocol is the Transmission Control Protocol (TCP). It lent its name to the title of the entire Internet Protocol Suite, *TCP/IP*. It is used for connection-oriented transmissions, whereas the connectionless User Datagram Protocol (UDP) is used for simpler messaging transmissions. TCP is the more complex protocol, due to its stateful design incorporating reliable transmission and data stream services. Other prominent protocols in this group are the Datagram Congestion Control Protocol (DCCP) and the Stream Control Transmission Protocol (SCTP).

There are many services that can be optionally provided by a transport-layer protocol, and different protocols may or may not implement them.

- **Connection-oriented communication**: It is normally easier for an application to interpret a connection as a data stream rather than having to deal with the underlying connection-less models, such as the datagram model of the User Datagram Protocol (UDP) and of the Internet Protocol (IP).
- Byte orientation: Rather than processing the messages in the underlying communication system format, it is often easier for an application to process the data stream as a sequence of bytes. This simplification helps applications work with various underlying message formats.
- Same order delivery: The network layer doesn't generally guarantee that packets of data will arrive in the same order that they were sent, but often this is a desirable feature. This is usually done through the use of segment numbering, with the receiver passing them to the application in order. This can cause head-of-line blocking.
- Reliability: Packets may be lost during transport due to network congestion and errors. By means of an error detection code, such as a checksum, the transport protocol may check that the data is not corrupted, and verify correct receipt by sending an ACK or NACK message to the sender. Automatic repeat request schemes may be used to retransmit lost or corrupted data.
- Flow control: The rate of data transmission between two nodes must sometimes be managed to prevent a fast sender from transmitting more data than can be supported by the receiving data buffer, causing a buffer overrun. This can also be used to improve efficiency by reducing buffer under run.
- Congestion avoidance: Congestion control can control traffic entry into a telecommunications network, so as to avoid congestive collapse by attempting to avoid oversubscription of any of the processing or link capabilities of the intermediate nodes and networks and taking resource reducing steps, such as reducing the rate of sending packets. For example, automatic repeat requests may keep the network in a congested state; this situation can be avoided by adding congestion avoidance to the flow control, including slow-start. This keeps the bandwidth consumption at a low level in the beginning of the transmission, or after packet retransmission.
- Multiplexing: Ports can provide multiple endpoints on a single node. For example, the name on a postal address is a kind of multiplexing, and distinguishes between different recipients of the same location. Computer applications will each listen for information on their own ports, which enables the use of more than one network service at the same time. It is part of the transport layer in the TCP/IP model, but of the session layer in the OSI model.

Connection management:

A symmetric connection management service between two service access points is specified, using a state transition system and safety and progress requirements. At each access point. the user can request connection establishment, request connection termination, and signal whether or not they are willing to accept connection requests from the remote user. The protocol can indicate connection establishment, connection termination, and rejection of a connection establishment request. The authors then specify a protocol and verify that it offers the service, given communication channels between the access points that can lose, reorder, and duplicate messages, but which guarantee delivery of a message that is repeatedly sent. The protocol achieves the service using 2-way and 3-way handshakes, and can be directly combined with any existing single-connection data transfer protocols to provide a transport layer protocol that offers both connection management and data transfer services.

Three way hand shaking:

Before the sending device and the receiving device start the exchange of data, both devices need to be synchronized. During the TCP initialization process, the sending device and the receiving device exchange a few control packets for synchronization purposes. This exchange is known as a three-way handshake.

The three-way handshake begins with the initiator sending a TCP segment with the SYN control bit flag set.

TCP allows one side to establish a connection. The other side may either accept the connection or refuse it. If we consider this from application layer point of view, the side that is establishing the connection is the client and the side waiting for a connection is the server.

TCP identifies two types of OPEN calls:

Active Open: In an Active Open call a device (client process) using TCP takes the active role and initiates the connection by sending a TCP SYN message to start the connection.

Passive Open: A passive OPEN can specify that the device (server process) is waiting for an active OPEN from a specific client. It does not generate any TCP message segment. The server processes listening for the clients are in Passive Open mode.

Session layers:

The session protocol defines the format of the data sent over the connections. Session layer establish and manages the session between the two users at different ends in a network. Session layer also manages who can transfer the data in a certain amount of time and for how long. The examples of session layers and the interactive logins and file transfer sessions. Session layer reconnect the session if it disconnects. It also reports and logs and upper layer errors.
The session layer allows session establishment between processes running on different stations.

Functions of Session layer:

- **Session establishment, maintenance and termination**: allows two application processes on different machines to establish, use and terminate a connection, called a session.
- **Session support**: performs the functions that allow these processes to communicate over the network, performing security, name recognition, logging and so on.

- **Protocols:** The protocols that work on the session layer are NetBIOS, Mail Slots, Names Pipes, RPC.

Presentation layer:

Presentation layer is also called translation layer. The presentation layer presents the data into a uniform format and masks the difference of data format between two dissimilar systems
The presentation layer formats the data to be presented to the application layer. It can be viewed as the translator for the network. This layer may translate data from a format used by the application layer into a common format at the sending station, and then translate the common format to a format known to the application layer at the receiving station.

Functions of Presentation layer:

- Character code translation: for example, ASCII to EBCDIC.
- Data conversion: bit order, CR-CR/LF, integer-floating point, and so on.
- Data compression: reduces the number of bits that need to be transmitted on the network.
- Data encryption: encrypt data for security purposes. For example, password encryption.

Application layer:

The application layer serves as the window for users and application processes to access network services. The application layer makes the interface between the program that is sending or is receiving data and the protocol stack. When you download or send e-mails, your e-mail program contacts this layer. This layer provides network services to the end-users like Mail, ftp, telnet, DNS.

Function of Application Layer:

- Resource sharing and device redirection.
- Remote file access.
- Remote printer access.
- Inter-process communication.
- Network management.
- Directory services.
- Electronic messaging (such as mail).

- Network virtual terminals.
- Protocols used at application layer are FTP, DNS, SNMP, SMTP, FINGER, and TELNET.

References:

1. [FOR] Behrouz A. Forouzan: Data Communication and Networking,
2. A.S.Tanenbaum,"Computer Networks",PHI
3. 3. J.F Hayes, Modeling and Analysis of Computer Communication Networks, Plenum Press
4. D. E. Comer, Internetworking with TCP/IP, Vol. I, Prentice Hall, India.
5. *www.notesdesk.com*
6. *www.webopedia.com*
7. *www.help.apple.com*
8. *www.mucins.weebly.com*
9. *www.en.wikipedia.org*
10. *www.sharmamonika95.blog.com*
11. *www.ecomputernotes.com*
12. *www.compnetworking.about.com*
13. *www.techterms.com*
14. *www.highteck.net*
15. *www.omnisecu.com*
16. *www.gurukpo.com*