Biyani's Think Tank

Concept based notes

Data Communication Network

MCA –II SEM

Ms Jyoti
Deptt. of IT
Biyani Girls College, Jaipur

Biyani's
Group of Girls' Colleges

Published by :
Think Tanks
Biyani Group of Colleges

Sector-3, Vidhyadhar Nagar,
Jaipur-302 023 (Rajasthan)
Ph : 0141-2338371, 2338591-95 • Fax : 0141-2338007
E-mail : acad@biyanicolleges.org
Website :www.gurukpo.com; www.biyanicolleges.org

Edition : 2012

Leaser Type Setted by :
Biyani College Printing Department

Preface

I am glad to present this book, especially designed to serve the needs of the students. The book has been written keeping in mind the general weakness in understanding the fundamental concepts of the topics. The book is self-explanatory and adopts the “Teach Yourself” style. It is based on question-answer pattern. The language of book is quite easy and understandable based on scientific approach.

Any further improvement in the contents of the book by making corrections, omission and inclusion is keen to be achieved based on suggestions from the readers for which the author shall be obliged.

I acknowledge special thanks to Mr. Rajeev Biyani, *Chairman* & Dr. Sanjay Biyani, *Director* (*Acad.*) Biyani Group of Colleges, who are the backbones and main concept provider and also have been constant source of motivation throughout this endeavour. They played an active role in coordinating the various stages of this endeavour and spearheaded the publishing work.

I look forward to receiving valuable suggestions from professors of various educational institutions, other faculty members and students for improvement of the quality of the book. The reader may feel free to send in their comments and suggestions to the under mentioned address.

Author

Syllabus

Overview, evolution of computer networks, computer telephony. Data communications – advantages of digital communication, transmission media, and fundament ales of digital communications, transmission media, modulation techniques and modems. The OSI seven layer network model, LAN technologies – protocols and standards, LAN hardware, TCP/IP and the Internet, Internet Architecture, Internet protocol and datagram., Routing protocols, UDP, Internet standard services, DNS. Networking Technologies, ISDN, Cable Modem System, DSL, SMDS, Frame relay, fast Ethernet, 100VG-anyLAN and Gigabit Ethernet, FDDI and CDDI, Asynchronous Transfer, SONET, DWDM Switching and Virtual LAN, Non-ATM Virtual LANs, IEEE 802.1Q VLAN standard, Network Performance, Analytical approaches, simulation, traffic monitoring. Network Management – SNMP, RMON and RMNv2, TMN, Directory services and network management. Issues related to network reliability and security, SSL and VPN, Introduction only to firewalls and Kerberos, Cyber Laws.

Content

UNIT 1 – Data Communication

- digital communication, advantages of digital communication
- communication, communication system
- Twisted pairs cable ,Advantages, disadvantages, uses ,types
- Coaxial cable, Advantages, disadvantages ,uses ,types
- Optical fiber cable, Advantages, disadvantages, uses, types
- transmission media, Advantages, disadvantages ,uses ,types
- modem, types of modems ,modulation
- data communication ,advantages ,disadvantages
- transmission mode, refraction

UNIT 2 – Network Protocol (OSI Model)

UNIT 3 – Networking Technologies

UNIT 4 -- Network Switching

UNIT 5 – Network Management

UNIT 6 – Network Security

Unit – 1

Data Communication

Q. 1 What is communication?

Ans. Communication is a layman language means to convey a message ,an idea, a picture or a speech that is received and understood clearly and correctly by the person for whom it is conveyed .There could be several methods of conveying the message.

Communication is sharing information have to be local or remote .Between individuals, local communication usually occurs face to face, while remote communication takes place or distance. the turn telecommunication ,which includes telephony, telegraphy and television, means communication at distance.

Telephonic communication is popular because it is cheap and instantaneous. We can talk to a person and convey a lot message on telephone, but picture cannot be sent on telephone . It is in this content ,that data communication containing messages, pictures and voices has taken the importance.

Definition : Data communication is the exchange of data (in the form of 0s and 1s)between two devices via some form of transmission medium(such as wire cable).Data communication is considered local if the communicating devices are in the same building or a similarly restricted geographical area, and is considered remote if the devices are farther apart.

Q. 2 What is communication system?

Ans. **Definition**--- Communication system is the combination of hardware, software and data transfer links that make up a communication facility for transferring data in a cost effective manner.

In the case of sending and receiving messages or data from one place to another, we have many elements working together All these elements put together to work efficiently is known as a system.

the communication system has the sole purpose of passing data or information in the most effective manner.

A communication system itself can be either analog or digital (or a combination of two). The information can be transmitted in either in analog from or in digital form within the communication networks. The technique by which a digital signal is converted to its analog form is known as modulation. The reverse processes, i.e. the conversation of analog signal to its digital form at the destination devices are called demodulation.

Q. 3 What are the advantages of digital communication?

Ans. Advantages of Digital communication:

(1) The voice data, music and images can be combined to make more efficient use of the same circuit and equipment.

(2) Much higher data transmission rates are possible using existing telephones lines.

(3) Digital communication is much cheaper than analog data transmission and also it is not necessary to accurately reproduce on analogue wave form after it has passed through potentially hundreds if reports a transcontinental call.

(4) Maintenance of a digital system is easier received correctly or not , making it simpler to track document the problems.

(5) A digital signals can pass through an arbitrary number of regenerators with no loss is signals and there travels long distances with no information loss.

Q. 4 Explain the following terms with their advantages and disadvantages ?

(a) Twisted pairs cable

(b) Coaxial cable

(c) Optical fiber cable

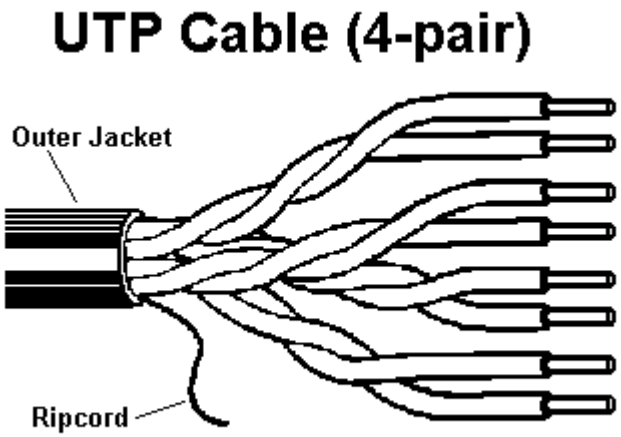
Ans. (a) TWISTED PAIRS:-- It has two types

- Unshielded twisted pair
- Shielded twisted pair

➢ Unshielded twisted pair:--A twisted pair consist of four insulated copper wires, typically about 1mm thick. The wires are twisted together in helical.

The purpose of twisting the curies is to reduce the electric interference from similar pairs close by.

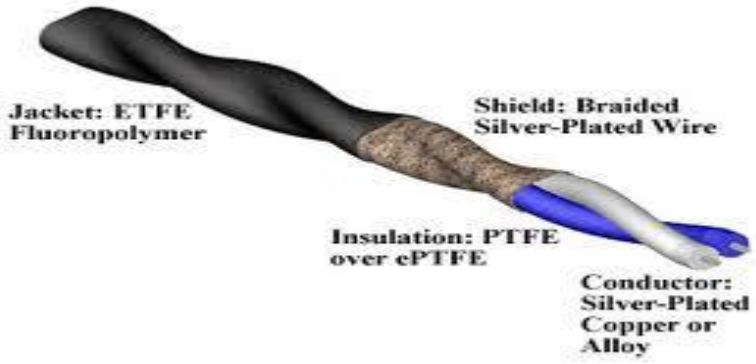
Twisted pair wires are commonly used for digital data transmission over short distances up to 1km.when many twisted pairs run in parallel for a substantial distance, such as all the wires coming from a multistory apartment building to the telephone exchange, they are bundled together and encased in a protective sheath. The pairs in these bundles would interface with one another. it wire not for the twisting.



UNSHEILDED TWISTED PAIR

- Shielded twisted pair:--Shielded wire is typically is used in an electrically noisy environment to limit the effects of noise absorption .unshielded pair commonly referred to as UTP is by far the more common of the two configuration twisted pair wiring is more commonly used for local area network.

  Twisted pair cabling comes in several varieties. Computer network ,true of these are important category-3 twisted pairs consist of two insulated wires gently twisted together .Four such pairs are typically grouped together in a plastic sheath for protection and to keep the eight wires together.



SHIELDED TWISTED PAIR

ADVANTAGES :---

1- Being the coldest method of data transmission trained manpower to repair and service this media of communication are easily available.
2- In a telephone system, signals can travel several kilometers without amplification when twisted pair wires are used.
3- This media can be used for both analog and digital data transmission. The bandwidth depends on the thickness of the wire and the distance travelled but several megabits per second can be achieved for a few kames, in many cases.
4- It is the least expensive media of transmission for short distances.
5- If position of a twisted pair cable is damaged, the entire network is not shut down as it may be case with coaxial cable.

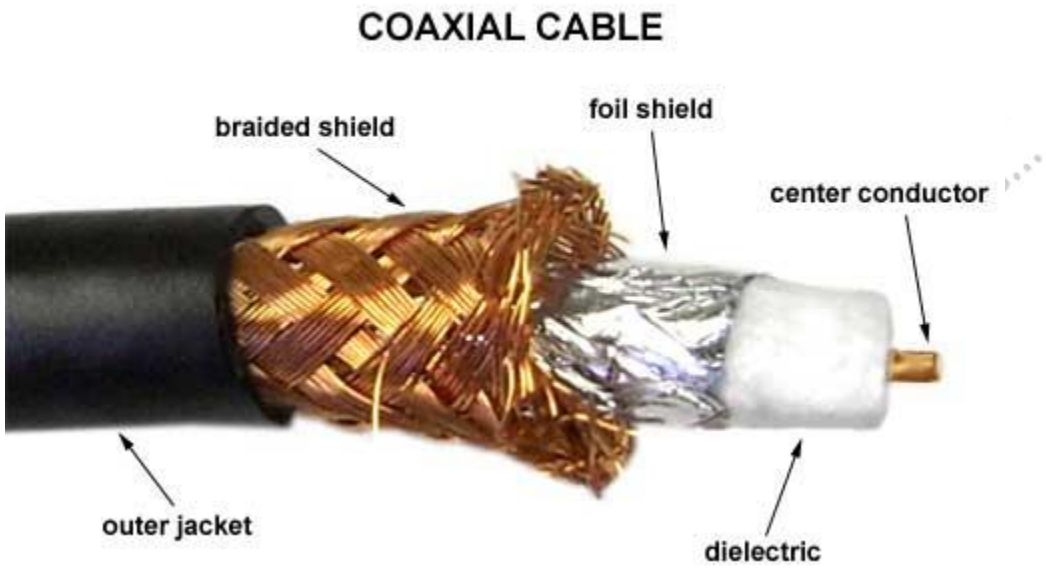
DISADVANTAGES: ---

1-Easily pick up noise signal which results in higher error rates when the line length exceeds 100meters.
2-Being thin in size, It is likely to break easily.

(b)COAXIAL CABLE:-- Coaxial cable consists of a shift copper wire as the core ,surrounded by an in insulating material. The insulator is encased by a cylindrical conductor often as a closely women braided mesh. The ought conductor is covered in an protective plastic sheath. The signal is transmitted by the inner copper wire and is electrically shielded by the outer metal sleeve. Two

kinds of coaxial cable are widely used .one kind 50-ohm cable is commonly used for digital transmission. The other kind, 75-ohm cables, is commonly used for analog transmission in cable TV transmission.

Coaxial cable is difficult to connect to network devices and generally requires more planning than twisted pair system. Many coaxial systems require the connectors on the main cable to be attached directly to the adapter on the PCs. This reduces flexibility in locating workstation and server.



ADVANTAGES:--

(a) It has better shielding than twisted pairs, so it can span longer distances at higher data bps.

(b) It can be used both analog data transmission as well as digital data transmission for analog ,75ohm.broadband coaxial is used and for digital data transmission 50ohm cable, baseband cable is used.

(c) Coaxial cable has higher bandwidth and excellent noise amenity.

(d) It is relatively expensive as ax pared to fiber optic cables and easy to handle.

(e) Coaxial cable has a bandwidth in the range of 300-400MHz,it is capable of carrying over 50 standard 6MHz color TV channels or thousand of channels of voice grade and 1 or low speed data over a single cable.

DISADVANTAGE:--

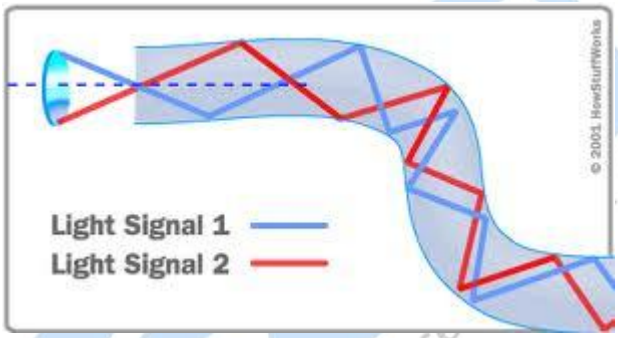
(a) Installation costs, while dropping, are still high.
(b) Special test equipment is often required.
(c) Susceptibility to physical damage.
(d) Wildlife damage to fiber optic cables.

(b) **OPTICAL FIBER: --** optical fiber is the newest form of bounded media .this media is superior in data handling and security characteristics .the fiber optic cable transmits light signals rather than electrical signals. it is for more efficient than the other network transmission media. Each fiber has an inner core of glass or plastic that conducts light.

There are two types of light sources for which fiber cables are available. These sources of light are:

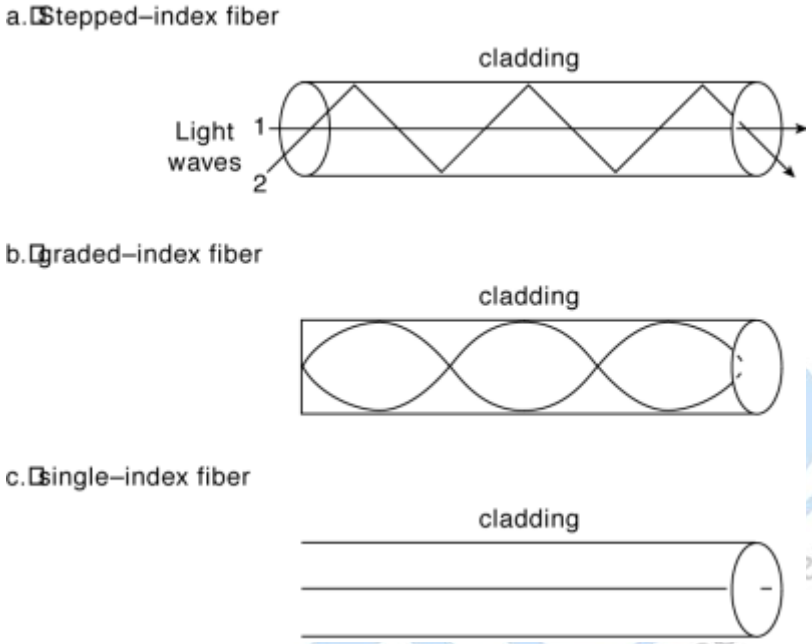
a- Light emitting diodes

b- Light amplification by stimulated emission radiation.

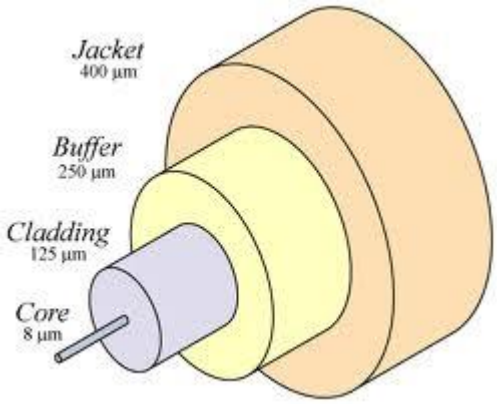


The system basically consists of fiber optic cables that are mode of tine threads of glass or plastic in a single mode fiber, the wire is 8 to 10 microns about the size of hair in multimode fibers, the core is of about 50microns in diameters.

Towards its sources side is a convert that converter that converts electrical signals into light waves. These light waves are transmitted over the fiber. Another converter placed near the sink converts the light waves back to electrical signals are amplified and sent to the receiver each fiber has a inner core of glass or plastic that conducts light. The inner core is surrounded by cladding. Cladding is layer of glass that reflects the light back in to the core.



Single mode fiber allows a single light path and is typically used with laser signaling. Single mode fiber can allow greater bandwidth than multimode but it is more expensive.



ADVANTAGES of fiber optic cable over copper wire:--

(a) It can handle much higher ban width than copper. Due to the low attenuation, repeats are needed only about every 30km on long lines, about every 5km for copper.

(b) Fiber is not being affected by power surges, electromegnatic interference or power failures. Nor it is affected by corrosive chemicals in the air, making it ideal for harsh factory environments.
(c) Fiber is lighter than copper.
(d) Fiber does not wake light and are quit difficult to tap. This gives an excellent security against potential wire tapper.

DISADVANTAGES of fiber optic cable over copper wire:--

(a) Fiber is an unfamiliar technology requiring skills most engineers do not have.
(b) Since optical transmission is inherently unidirectional ,two ways communication requires either two fibers of fours frequency bands on one fiber.
(c) fiber interfaces cost more than electrical interfaces.

Q. 5 Explain transmission media ?

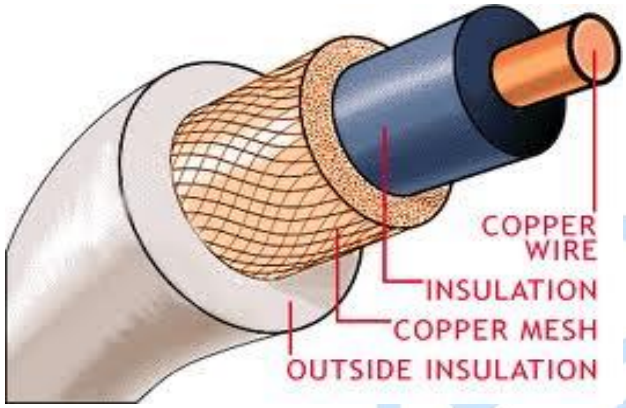
Ans Transmission media :-media is the general term used to describe the data path that forms the physical channel between sender and the receiver.media can be twisted pair wire such as that used for telephone installation ,coaxil cabel of various sizes and electrical characterstics, fiber optics and wireless supporting either light waves or radio waves.
Band width is similar to the concept of frequence response in a stereo amplifier— the greater the frequance response, the higher the band width according to a fundamental princepal of information theory ,higher band width communication channels support higher data rates.

Q.6 Explain the types of transmission media ?

Ans There are several types of physical channels (communication media)through which data can be transmitted from one point to another .some of the most common data transmission media are as follow :--

- Guided media
  - **electrical**
    - Twisted pair cable
    - coaxial cable

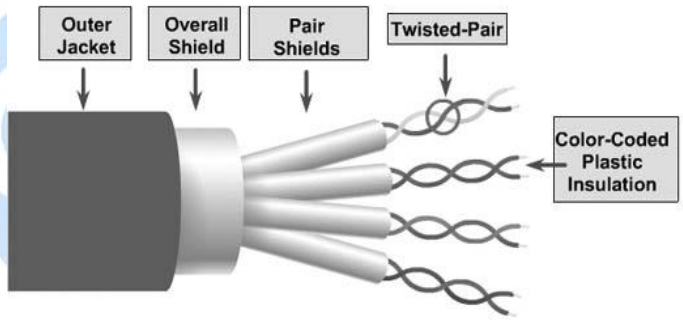
- **optical**
  - single mode and multimode



coaxial cable

➢ **Unguided media**

- electromagnetic waves in air
  - radio
  - microwaves



Twisted Pair

Various forms of data path can be used depend on the type of coputers connected and the data rate.i.e number of bits passed in one second.there are thus main types of communication media.these are bounded and unbounded media.in the case of boundedmedia,the data is transferred in the limited space whereas in the case of unbounded media,there is no restriction on the space.

Q.7 What is modulation?

Ans Modulation is the method of mixing intelligent signal on to the carrier signal so that a weak intelligent signal can be transmitted over long distance over a transmission media such as copper conduct or coaxial cable. Modulation is the process of converting a digital signal from a computer into an analog signal the telephone system will accept .when you pick up the phone while your computer modem is communicating .

Q.8 Explain the concept of modulation ?

Ans Concept of modulation :

Due to the fact that both attenuation and propagation of speed are frequency dependent ,it is undesirable to have a wide range of frequencies in the signal but square waves in digital data have a wide spectrum and are subject of strong attenuation and delay distortion.

Modulation is to mix a data signal onto a carrier and modify its characteristics for transmission in a communication network. A carrier is electromagnetic wave that vibrates at a fixed frequency.

Data modulate by carrier by various methods .and these methods are :

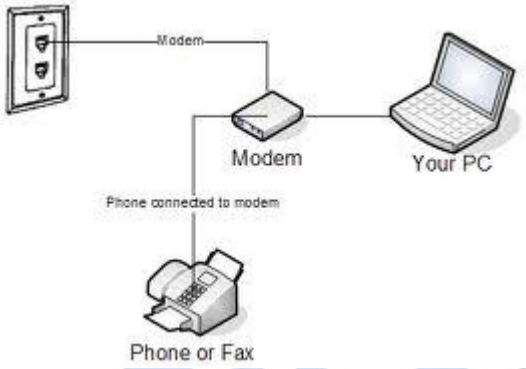
(a) amplitude modulation
(b) frequency modulation
(c) phase modulation

Q.9 What is modem ?

Ans **M**odem stands for modulator demodulator. Modems convert communication signals from a form the computer can understand to aform the telephone system can convey and vice versa.

Modems convert communications signals from a form the computer can understand to a form the phone system can convey and vice versa .modems speed is often discussed in baud rates or bps , which are similar terms but they do not mean exactly the same baud rate refers to the oscillation of a sound wave on which a single bit of data is carried. bits per second is the amount of data transferred in a second.

When a computer wishes to send digital data over a dial up line ,the data must first be converted to analog form by a modem for transmission over the local loop ,then convert to digital form for transmission over the long –haul trunks ,then back to analog over the local loop at the receiving end.



MODE

A modem can be installed internally in the computer in which case it is called an internal modem ,or it can be a external device that is connected to the computer with a serial cable.

Q.10 Explain the types of modems ?

Ans Modems can be of following types :

(a)Landline modems

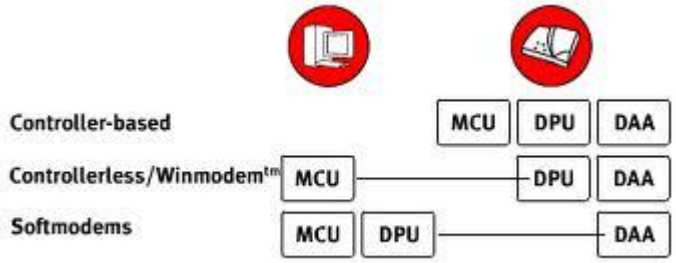
(b)wireless modems

(c)LAN modems

=> Landline modems are modems which connect to the public switched telephone network (PSTN).to connect to PSTN, these modems have have a jack known as RJ-11jack or regular phone jack.
Landline modems can be further classified into the following types :
(a)internal modems
(b)external modems
(c)PCMCIA modems
(d)voice/data/modems

=>wireless modems are redio transmitters/receivers installed into mobile computing devices(i.e.devices that are used while you are moving such as mobile phones,laptops etc)

=>Lan modems allow shared remote access to lan resources.lan modems comes fully preconfigured for asingle particular network architecture such as Ethernet or token ring.



LAN

Q.11 Explain the modem standards ?

Ans There are two modem standards .these are :
(a)**B**ell modems
(b)ITU-T modems
First commercially available modems were developed by Bell telephone company in the early 1970s.Being the first modem manufacturer, they defined the developed of the technology and provided the standard which subsequent manufactures followed. some major Bell modems include the 103/113series,202series,212series,201series.
Many of today's popular modems are based on the standards published by ITU-T.v.21,v.22,v.23,v.32 modems are ITU-T modems.

Q.12 What are the advantages of data communication ?

Ans **D**ata communication has a following advantages :

(a) Pictures sound and written data can be sent within minutes and a confirmation about it reaching at the destination can be obtained indirectly.

(b) Message can be coded so that it is not understood by anybody else except the person who is sending and the person who is receiving the message. even if the message is intercepted on the way, it can not be decoded.

(c) Message can be sent in any language including hindi, regional language or european language from any part of the world to any other part of the world.

(d) Users need not take highly specialized training for sending or receiving messages.

(e) In addition waying to conveying a message ,the same pc can also be used as an instrument to get information from varied sources such as railways ,stock exchange. even goods can be purchased using computers and is return the payments can be sent electronically.

(e) PCs connected with modem can also be used for education,entertainment,etc.

(f) Telephonics calls can be made to any part of the world with the same expenses as a local telephone call made within the city.

Q.13 What are the main components of data communication ?

Ans Components of the data communication :

1- **Messages:--** the messages is the information (data)to be communicated.it can consist of text,numbers,pictures,sound on video or any combination of these.

2- **Sender**:-- the sender is the device that sends the data message.it can be a computer workstation,telephone handset video camera and so on.

3- **Receiver:--** the receiver is the device that recevices the messages .it can be a computer,workstation,handset
Telephone and so on.

4- **Medium:--** the transmission medium is the physical path by which a message travels from sender to receiver.it can consist of twisted pair wire,cables,fiber,optic cable,laser or radio weaves.

5- **Protocol:--** a protocol is a set of rules that govern data communication devices.without a protocol ,two devices may be connected but not communicating,just as a person speaking french can not be understand by a person who speaks only japanese.

Q.14 Define data communication network ?

Ans Data Communication network :--the task of network designers is to selected and coordinate the network components is that the necessarydata are module to the right place,at the right time,with minimum of errors and at the lowest possible cost.a number of communication processor are used by network designers to achieve this goal.

Communication system is the combination of hardware,software and data transfer units that make up a communication facility for transferring data in an efficient manner.

Q.15 What are the characteristics of data communication system ?

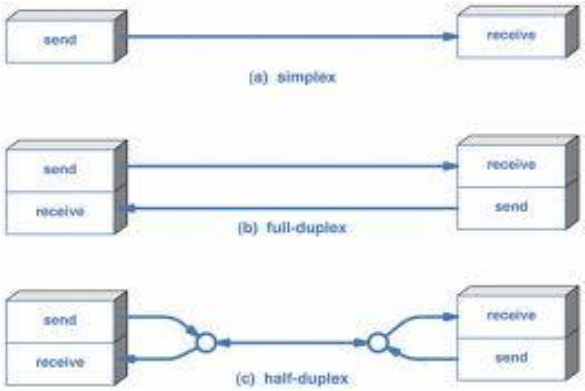
Ans Fundamentals characteristics of data communication system :

1- **Delivery**: the system must deliver data to the correct destination.data must be received by the intended devices or user and only by that device or user.
2- **Accuracy**: the system must deliver data accuratly. data that have been altered in transmission and left uncorrected are unusable.
3- **Timeliness**: the system must deliver data in a timely manner data delivered late are useless. in the case of videos, audios, and voice data. timly deliverly means delivering data as they are produced in the same order that they are produced and without significant delay. this kind of delivery is called real time transmission.

Q.16 Write down the transmission mode ?

Ans The term transmission mode is used to define the direction of signal flow between two linked devices.there are three types of transmission modes :

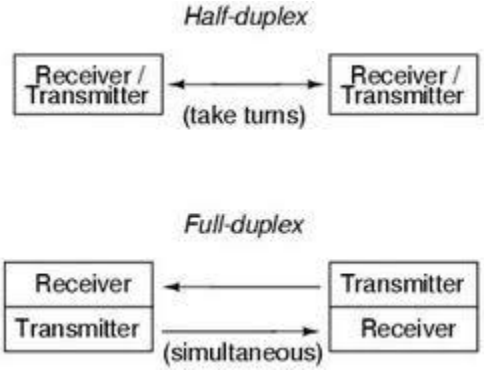
1- Simplex
2- Half-duplex
3- Full-duplex



1- **SIMPLEX** :--in this mode,the communication is undirectional,as on a one-way communication transmission.television transmission is avery good example of simplex communication.the main transmitter sends out a signal(broadcast),but it does not expect a reply as the receving units can not issue reply back to the transmitter.exam: include a data collection terminal one a factory floor or a line printer.

2- **HALF-DUPLEX** :-- in half-duplex mode,both units communicate our same medium,but only one unit can send at a time.while one is in send mode,the other unit is in receiving mode.it is like true polite people talking to each other-one talk the other listen,but both of them could not talk at the same time –thus a half duplex line can alternately sen and receive data.it requires two wires it is used to connect a terminal with computer.the terminal might transmit data and them the computer responds with an acknowledgement.the transmission of data to and from a hard disk is also done in half duplex mode.

3- **FULL-DUPLEX**:-- a half-duplex system,the line must be "turned around "each time the direction is requires. This involves a special switching circuit and requires a small amount of time with high speed capabilities of the computer this turn around time is unacceptable in many instances. also,some application requires simultaneously transmission in both direction in such cases a full duplex system is used that allows information to flow simultaneously in both direction on the transmission path. use of full-duplex line improves efficiency as the line turnaround time required in a half-duplex arrangement is eliminated also requires four wires for full-duple.



Q.17 What is REFRACTION ?

Ans Refraction:--light travel in a straight line as long as it is moving through a single uniform substance. If ray of light travelling through one substance suddenly enters another substance, its speed changes abruptly, causing the ray to change direction. This change is called refraction.

The two angles mode by the beam refraction in relation to the vertical axis are called I for incident and R for refracted the beam travels from a less dense medium into a more sense medium. In the case angle angle R is smaller than angle I.

When a beam travels from a more dense, medium into a less dense medium. in this case the value of I is smaller than the value of R, when light travels into denser medium, the angle of incidence is grater than the angle of refraction.

Unit– 2

Network Protocol (OSI Model)

Q.1 What is OSI model ?

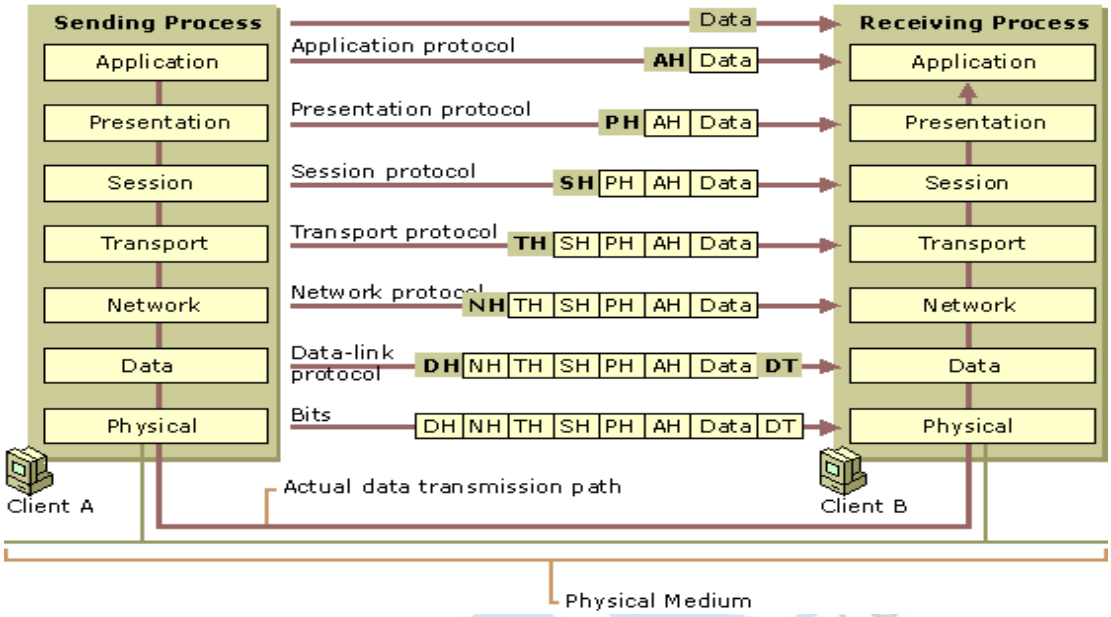
Ans Model :-- The OSI model is layered framework for the design of network system that allows for communication across all types of computer system .it consist of separate but related layers, each of which defines a segment of the process of moving information across a network.

Q. 2 Explain the architecture of OSI seven layer network model ?

Ans LAYER Architecture :--The OSI model is built of seven ordered layer :

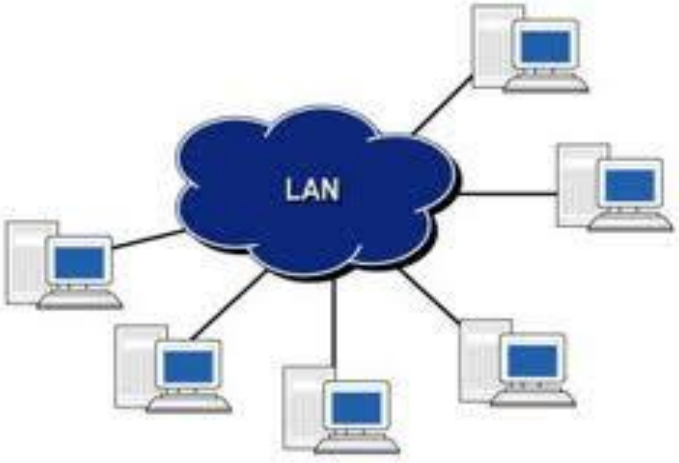
1- Physical layer
2- Datalink layer
3- Network layer
4- Transport layer
5- Session layer
6- Presentation layer
7- Application layer

The message is passed into many intermediate nodes(a to b mod)



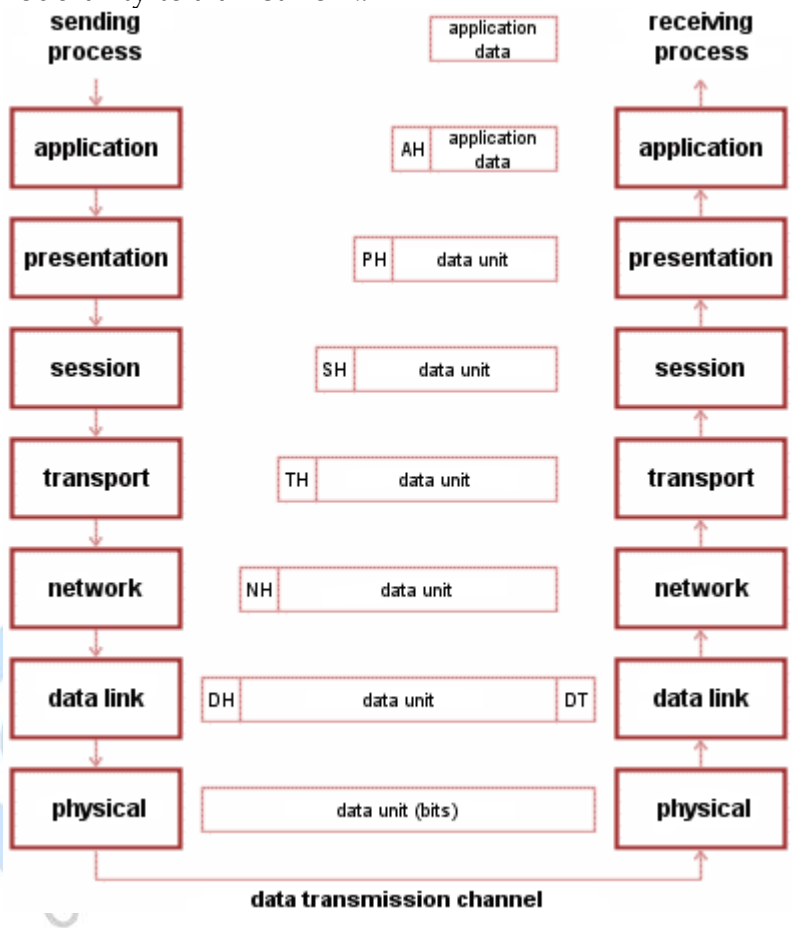
Q.3 What is LAN ?

Ans Local area network(LAN) is a group of computer located in the same room, on the same floor, or in the same building that are connected to form a single computer network .local area network allows users to share storage devices, printers , applications, data and other network resources.



Q 4 What is interfaces between layer ?

Ans Interfaces between layers:--the passing of the data and network information down through the layers of the sending machine and back up through the layers of the receiving machine is made possible by an interface between each pair of adjacent layers .each interfaces defines what information and services a layer must provided for the layer above it well defined interfaces and layer function provide modularity to a a network.



Q5 Explain pair to pair process ?

Ans Pair to pair process:--between machines , layers x on one machine communicates with layer x on another machine. This communication is governed by an agreed upon series of rules and convention called protocols. The processes on each machine that communicates at a given layer are called pair-to-pair process. Each layer in the sending machine adds its even information to the message it receives

from information is added in the form of header or trilers, headers are added to the message at layer 6,5,4,3,2 a trailor is added at layer 2.

Q6 Explain the organization and function of the OSI layers ?

Ans Organization of the layer :--

The seven layer can be thought of as belonging to three subgroups, layers 1,2and 3-physical, datalink layer and network –are the network support layers ,they deal with the physical aspects of moving data from one devices to another.layer5,6,7-session , presentation and application can be thought of as the user support layers; they allow interoperability among unrelated software system. layer 4,the transport layer, ensure end to end reliable data transmission while layer 2 ensures reliable transmissions on a single link, the upper OSI layer are almost always implemented in software.

Function of the layers :--

- PHYSICAL Layer :
  1- The physical layer coordinates the functions required to transmit a bit stream over a physical medium.
  2- It deals with the mechanical and electrical specification of the interfaces and transmission medium.
  3- It also defines the procedures and function that physical devices and interfaces have to perform for transmission to occur.

4- It defines the actual set of wires,plugs and electrical signals that connect the sending and receiving devices to the network.

FEATURES :

1- Physical characteristics of interfaces and media : the physical layer defines the characteristics of the interface between the devices and the transmission medium.

2- Representation of bits : the physical layer data consist of a stream of bits without any interpretation.

3- Data rate : the transmission rate—the no of bits sent each second is also defined by the physical layer.

4- Synchronization of bits :the sender and receiver must be synchronized at the bit level.

5- Line configuration : in a point to point configuration,two devices are connected to gether through a dedicated link.

6- Physical topology : the physical topology defines how devices are connected to make a network.

7- Transmission mode : the physical layer also defines the direction of transmissions between four devices.

- **DATA LINK LAYER**

1- The data link layer transform the physical layer ,a row transmission facility,to a reliable link and is responsible for node to node delivery.

2- It makes the physical layer appear error free to the upper layer(network).

- Responsibilities:

1- Framing :-- the data link layer divides the steam of bits received from the network layer into manageable data units called frames.

2- Physical addressing :-- if frames are used to be distributed to different system on the network,the data link layer adds a header to the frame to define the physical address of the sender (source add.)and or receiver destination address of the frame.

3- Flow-control :--if the rate at which data are absorbed by the receiver is less than the rate produced in the sender ,the data link

layer impose a how control mechanism to prevent overhelming the receiver.

4- Error control :--the data link layer adds reliability to the physical layerby adding mechanism to detect and retransmit damaged or lost frames.

5- Access control :--when four or more devices are connected to the same link ,data link layerprotocols are necessary to determine which devices has control our the link at any given time.

- **Network layer :--**

1- This is responsible for the source to destination delivery of a packet possibly across multiple networks.

2- The network layer ensures that each packets get from its point of origin to its final destination.

3- If thus system are connected to the same link there is usually were need for a network layers.

4- The two systems are attached to different networks (links)with connecting devices between the network ,there is often a need for the network layer to accomplish source-to-destination delivery.

- Responsibilities:

1- Logical addressing :--the network layer adds a header to the packet coming from the upper layer that ,among other things,includes the logical addresses of the sender and receiver.

2- Routing :-- when independent networks or links are connected together to create an internetwork ,the connecting devices called router or gateways,route the packets to their final destination.

- **TRANSPORT Layer :--**

The transport layer breaks large messages from the session layer into packets to be sent to the destination computer and ressembles packets into messages to be presented to the session layer.the transport layer typically sends an acknowledgement to the originator for the messages received.

- **Responsibilities:**

1- Service –point addressing:-- the transport layer header therefore must include a type of address called a service point address. The network layer gets each packet to the correct computer .the transport layer gets the entire messages to the correct process on that computer.
2- Segmentation and reassembly:--a message is divided into transmittable segments each segment containing a sequence number. This number enables the transport layer to reassemble.
3- Connection control:--the transport layer can be either connectionless or connection oriented.
4- Flow control:--flow control at this layer is performed end to end rather than across a single link.
5- Error control: -- error control at this layer is performed end to end rather than across a single link. The sending transport layer without error (damaged, loss, duplication).

- **SESSION layer**:-- the session layer is the network dialog controller .it establishes, maintains and synchronizes the interaction between communicating systems.
  - **Responsibilities:**
    1- Dialog control:- the session layer allows two systems to enter into a dialog. It allows the communication between two processes to take places either in half duplex or full duplex.
    2- Synchronization:--the session layer allows a process to add checkpoints into a stream of data.
- **PRESENTATION layer**:--It is concerned with the syntax and semantics of the information exchanged between two systems. The presentation layer translates data between the formats the network requires and the formats the translations.

Note: The presentation layer adapts information to the local environment.

- Responsibilities:
  1- Translation:--the process in two system are usually exchanging information in the form of character strings, numbers and so on

.the information should be changed to bit stream before being transmitted.

2- Encryption:--it means that the sender transform the original information to another form and sends the resulting message out over the network.

3- Compression:--data compression reduces the number of bits to be transmitted. It is important for multimedia searches text,audio,or video.

- **APPLICATION layer :--**it is the top most layer of the OSI model.It enables the user whether human or software, to access the network .it provides the user interfaces and support for services such as electronic mail, remote file access and transfer shared database management and other types of distributed information services.
  - **Responsibilities:**
    1- Network virtual terminal:--it is a software version of a physical terminal and allows a user to log on to a remote host. The remote host believes it is communicating with one of its own terminal and allows you to log on.
    2- File transfer, access and management :--this application allows a user to access files in a remote computer, to retrieve files from a remot computer and to manage and control files in a remote computer .
    3- Mail service:--this application provides the basis for e-mail forwarding and storage.
    4- Directory service:--this application provides distributed database sources and access for global information about various objects and services.

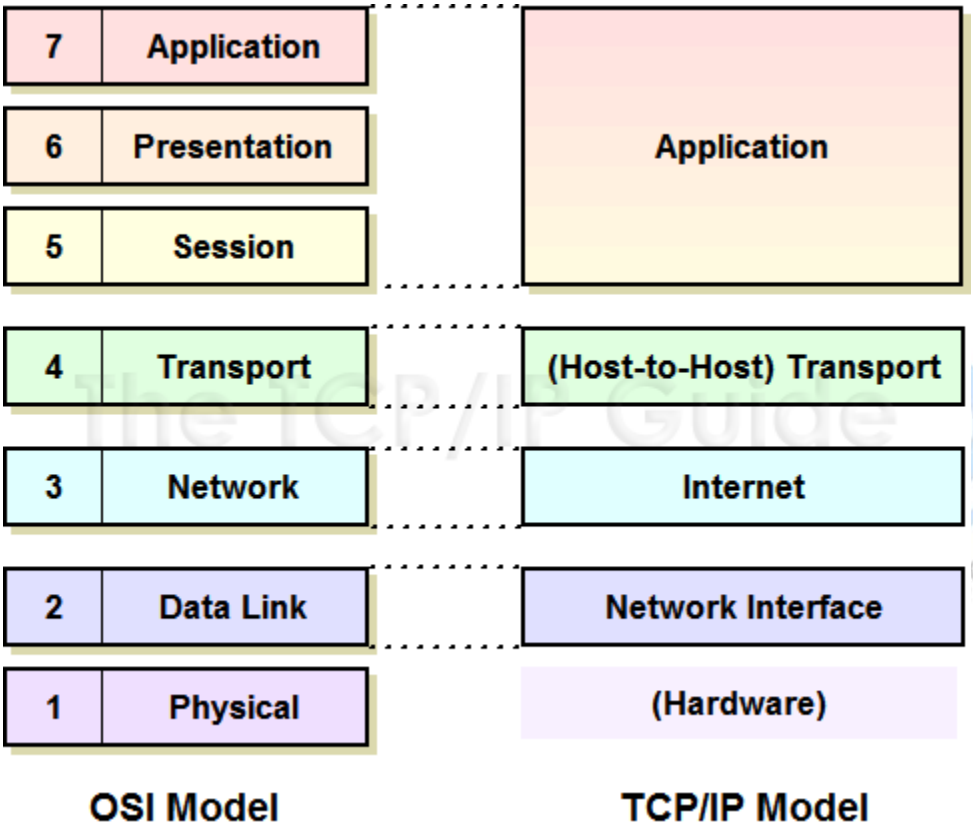
Q 7 Explain TCP/IP ?

Ans TCO/IP:-- The Internet protocol suite is the set of communications protocols used for the Internet and similar networks, and generally the most popular protocol stack for wide area networks. It is commonly known as TCP/IP, because of its most important protocols: Transmission Control Protocol (TCP)

and Internet Protocol (IP), which were the first networking protocols defined in this standard. It is occasionally known as the DoD model due to the foundational influence of the ARPANET in the 1970s (operated by DARPA, an agency of the United States Department of Defense).

TCP/IP provides end-to-end connectivity specifying how data should be formatted, addressed, transmitted, routed and received at the destination. It has four abstraction layers, each with its own protocols. From lowest to highest, the layers are:

1. The link layer (commonly Ethernet) contains communication technologies for a local network.
2. The internet layer (IP) connects local networks, thus establishing internetworking.
3. The transport layer (TCP) handles host-to-host communication.
4. The application layer (for example HTTP) contains all protocols for specific data communications services on a process-to-process level (for example how a web browser communicates with a web server).



Q 8 What is internet protocol ?

Ans INTERNET PROTOCOL :--(ip)works at the network layer .the Functions it handle and methods it uses are as follows:

(a) For addressing, it uses the logical network address.
(b) For switching purpose, it uses the packet switching method.
(c) For route selection, it uses the dynamic method.
(d) For connection services, it provides error control.

IP is connectionless, datagram protocol (ip packets are also reffered to as ip datagram)ip uses packet switching and perform route selection by using dynamic routing tables that a referenced at each hop. The packets making up a message could be routed differently through the internetwork depending on the

state of the network at each hop. For example, if a link were to go down or become congested, packet will be sent through a different route.

Appended to each packet is an ip header, which includes sources and destination information. ip uses sequence numbering if it is necessary to fragment a packet into smaller parts and reassembles it at its destination or at an intermediate point. ip performs error checking on the header information by way of a checksum.

IP addresses are unique, 4byte addresses that must be assigned to every addressable device or node on the internetwork .a big message is divided into smaller packets by the TCP. These are given a header and then enveloped by the ip to be sent to the addresses by various routes using the router at the receiving end each envelop is placed in order and the message is reassembled by the TCP and forwarded to the addresses.

Q9 What is DNS ?

Ans DNS stands for Domain Name System. Sun Microsystems developed the domain Name System

(DNS) in the early 1980s as an easier way to keep track of Internet addresses .The DNS establishes a hierarchy of domains, which are groups of computers on the Internet.

The DNS gives each computer on the net an Internet address or domain name, using easily recognizable letters and words instead of numbers.

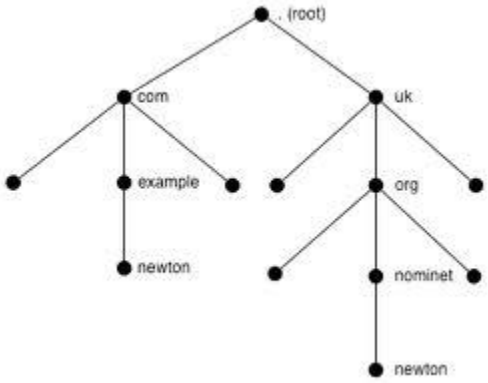
Domain Nmae System (DNS) is the standard for resolving names to Internet addresses. However, the hosts file still plays a role in name resolution during LAN resolution when DNS is down. In a nutshell, DNS is a distributed database whose structure looks system in which like the UNIX file system. DNS is a client/server system in which the resolvers query the named servers to find an address record for a domain name. The query process begins with the root name servers. If the root name server does not know the answer, it returns the address of a name server, This iterative process continues until a name server respond with the address for the domain name.

Q.10 Explain the types of DNS?

Ans The root of DNS database on the Internet is managed by the INTERNET Network Information Center(http://www.internic.com).

The top-level domains were assigned organization wise, and by country. DNS is a protocol that can be used in different platforms . In the Internet, the domain name space(tree) is divided into the three different sections:

(a) Generic domains
(b) Country domains
(c) Inverse domains



DNS ZONES

Generic Domains:

The generic domains define registered hosts according to their generic behavior. Each node in the tree defines a domain, which is an index to the domain name space database. The first level in the generic domain section allows seven possible three character labels. These labels describe the organization types as listed in Table:

Generic domain names

Label	Description
Edu	Educational Organizations
Com	Commercial Organizations

Country Domains:

The country domains section follows the same format as the generic domains but uses two-character country abbreviations (e.g., "us" for United States) in palce of the three- character organizational abbreviations at the first level. Second level labels can be organizational, or they can be more specific, national destinations.

The United states for example, uses state abbreviations as a subdivision of "us" (e.g., ca.us.).

Inverse Domain : The inverse domain is used to map an address to a name . This may happen, for example, when a server has received a request from a client to do a task. Whereas the server has a file that contains a list of authorized clients(extracted from the received IP packet). To determine if the the client is on the authorized list, it can send a query to the DNS server and ask for a mapping of address to name.

Q.11 What is UDP ?

Ans UDP(user datagram protocol)is a connectionless protocol that works at the transport layer.UDP transports datagram's but does not acknowledge their receipt .UDP also uses a port address to achieve datagram delivery ,but this port address is simply a pointer to a process ,not a connection identifier ,as it is with TCP. The lack of overhead makes UDP faster than TCP .hence a sender whishing to send a small message and does not care much about reliability can use UDP.

UDP provides no flow control or acknowledgements for received packets. If UDP detects some error while transmitting a datagram, it simply drops the datagram and does not inform the sender about the same.

Q.12 Explain UDP applications?

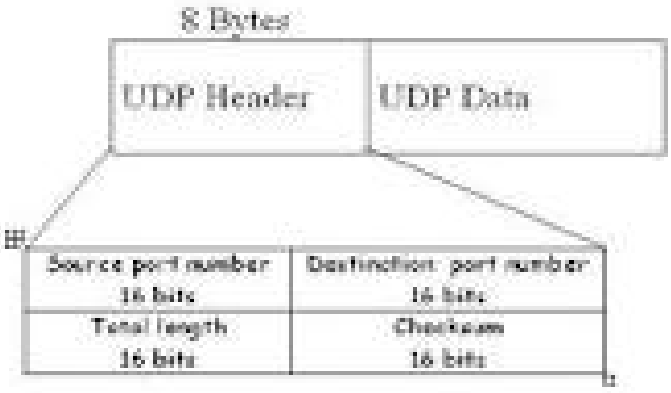
Ans UDP applications : The following are some applications of UDP Protocols-

(a) UDP is used for simple request response communication.

(b) UDP is only suitable for a process having internal flow and error control mechanisms such as TFTP(trivial file transfer protocol).

(c) UDP is suitable transport protocol for multicasting and broadcasting.

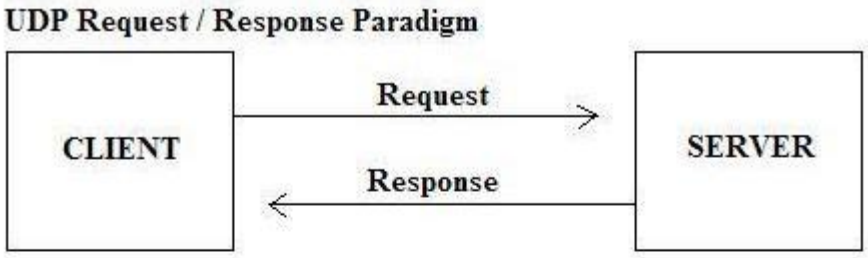
(d) UDP is applied for route updating protocols namely, routing information protocol.

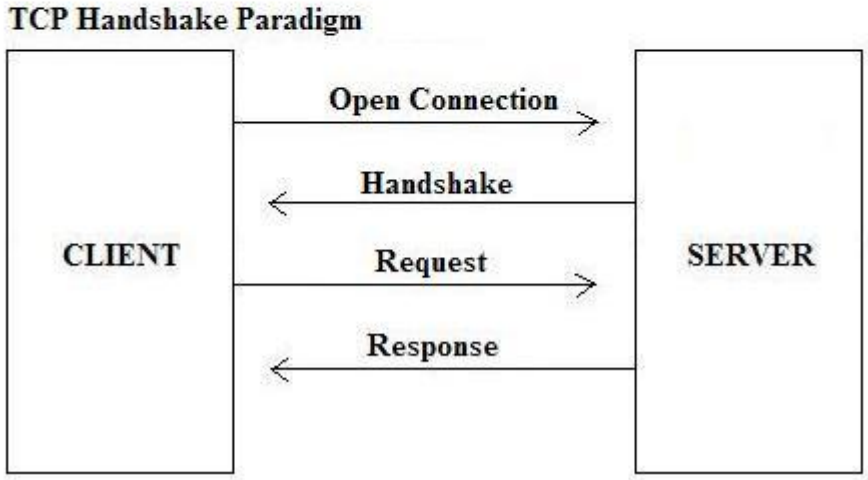


Q.13 How UDP works ?

Ans UDP gives a connectionless services each user datagram's sent by udp is an independent datagram. There is no relationship between the various user datagram's even when they are coming from the same source process and going to the same destination program .the user datagram's are not numbered moreover , each user datagram can travel a different path.

Each request must be small enough to fit into one user datagram .only some processor sending short message need to use UDP because it cannot cut messages into small segments.





Encapsulation and decapsulation of messages

Following are the steps for sending messages using UDP:

(a) If processor has a message to send through udp,it passes the message to udp along with a pair of socket addresses giving the length of data.

(b) Udp receives the data .it adds the udp header.
Udp then passes the user datagrams to the ip with the socket addresses.

(c) Ip adds its own header indicating that the data has come from the udp protocol.the ip datagram is then passed to the data link layer .

(d) The data link layer receives the ip datagram.it adds its own header and passes it to the physical layer.

(e) The physical layer encodes the bits into electrical or optical signals and sends it to the remote machine.

(f) When the message arrives at the destination host ,the physical layer decodes the signals into and passes it to the data link layer.

(g) The data link layer uses the header and the trailer to check the correctness of data. if there is no error ,the header and the trailer are dropped and the datagram is passed to the ip.

(h) The ip software does its own checking .if there is no error ,the header is dropped and the user datagram passed to the udp with the sender and receive ip addresses

(i) Udp uses the checksum to check the entire user datagram .if there is no error, the header is dropped and the application data along with the sender socket address is passed to the process.

(j) The sender socket address is passed to the message received.

At the server site ,the mechanism of creating queues is as follows :

(a) A server asks for incoming and outing queues using its well known port when it starts running the queues remain open as long as the server is running.

(b) When a message arrives for a server , udp checks to see if an incoming queue has been created for the port number specified in the destination port number field of the user datagram.

(c) If there is a queue , udp sends the received user datagram to the end of the queue.

(d) If there is no such queue , udp discards the user datagram and ask the ICMP protocol to send a port unreachable message to the client.

(e) If queue is overflows then udp drops the user datagram .it asks for a port unreachable message to the client .

(f) When a servant wants to respond to a client it sends messages to the outgoing queue using the source port number specified in the request.

(g) Udp removes the messages one by one ,and after adding the udp header ,delivers them to ip.

(h) In case ,an outgoing queue overflows then operating system asks the server to wait before sending any more messages.

Q. 14 What is Datagram?

Ans A datagram is a packet that is sent over a network using a connectionless service ,i.i. a network where the delivery of data does not depend on the maintenance of connections between the communicating computers. Such service do not

guarantee that the datagrams will be delivered without error, without duplication or loss and in the same serial order in which they were sent. They only guarantee a "best effort" delivery of datagram.
Packets in the ip layer are called datagram.a datagram is a variable length packet (up to 65,536bytes) consisting of two parts
(a) Header
(b) data

Q.16 What is internet ?

Ans The Internet is a global system of interconnected computer networks that use the standard Internet protocol suite (often called TCP/IP, although not all applications use TCP) to serve billions of users worldwide. It is a network of networks that consists of millions of private, public, academic, business, and government networks, of local to global scope, that are linked by a broad array of electronic, wireless and optical networking technologies. The Internet carries an extensive range of information resources and services, such as the inter-linked hypertext documents of the World Wide Web (WWW) and the infrastructure to support email.

Most traditional communications media including telephone, music, film, and television are reshaped or redefined by the Internet, giving birth to new services such as Voice over Internet Protocol (VoIP) and Internet Protocol Television (IPTV). Newspaper, book and other print publishing are adapting to Web site technology, or are reshaped into blogging and web feeds. The Internet has enabled and accelerated new forms of human interactions through instant messaging, Internet forums, and social networking. Online shopping has boomed both for major retail outlets and small artisans and traders. Business-to-business and financial services on the Internet affect supply chains across entire industries.

The origins of the Internet reach back to research of the 1960s, commissioned by the United States government in collaboration with private commercial interests to build robust, fault-tolerant, and distributed computer networks. The funding of a new U.S. backbone by the National Science Foundation in the 1980s, as well as private funding for other commercial backbones, led to worldwide participation in the development of new

networking technologies, and the merger of many networks. The commercialization of what was by the 1990s an international network resulted in its popularization and incorporation into virtually every aspect of modern human life. As of 2011, more than 2.2 billion people – nearly a third of Earth's population — use the services of the Internet.

The Internet has no centralized governance in either technological implementation or policies for access and usage; each constituent network sets its own standards. Only the overreaching definitions of the two principal name spaces in the Internet, the Internet Protocol address space and the Domain Name System, are directed by a maintainer organization, the Internet Corporation for Assigned Names and Numbers (ICANN). The technical underpinning and standardization of the core protocols (IPv4 and IPv6) is an activity of the Internet Engineering Task Force (IETF), a non-profit organization of loosely affiliated international participants that anyone may associate with by contributing technical expertise.

Q.17 Explain internet standard and internet architecture ?

Ans A specification for which at least two independent and interoperable implementations and successful operational experience has been obtained may be elevated to the Internet Standard level. An Internet Standard is characterized by a high degree of technical maturity and by a generally held belief that the specified protocol or service provides significant benefit to the Internet community.

Generally Internet Standards cover interoperability of systems on the Internet through defining protocols, messages formats, schemas, and languages. The most fundamental of the Internet Standards are the ones defining the Internet Protocol.

All Internet Standards are given a number in the STD series - The first document in this series, STD 1, describes the remaining documents in the series, and has a list of Proposed Standards.

Each RFC is static; if the document is changed, it is submitted again and assigned a new RFC number. If an RFC becomes an Internet Standard (STD), it is assigned an STD number but retains its RFC number. When an Internet Standard is updated, its number stays the same and it simply refers to a different RFC or set of RFCs. A given Internet Standard, STD n, may be RFCs x and y at a given

time, but later the same standard may be updated to be RFC z instead. When STD 1 is updated again, it will simply refer to a newer RFC, but it will still be STD 1. Note that not all RFCs are standards-track documents, but all Internet Standards and other standards-track documents are RFCs.

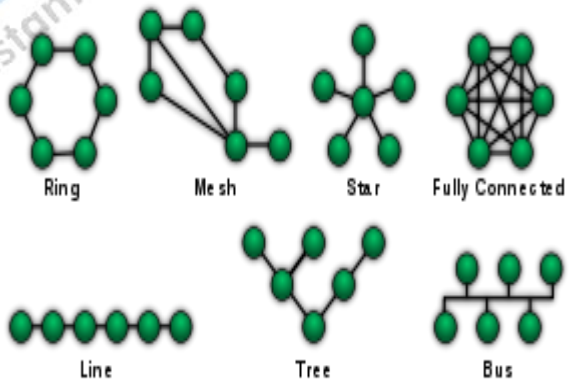
Q.18 Explain network topologies and their types ?

Ans **Network topology** is the arrangement of the various elements (links, nodes, etc.) of a computer or biological network. Essentially, it is the topological structure of a network, and may be depicted physically or logically. *Physical* topology refers to the placement of the network's various components, including device location and cable installation, while *logical* topology shows how data flows within a network, regardless of its physical design. Distances between nodes, physical interconnections, transmission rates, and/or signal types may differ between two networks, yet their topologies may be identical.

Logical topologies are often closely associated with Media Access Control methods and protocols. Logical topologies are able to be dynamically reconfigured by special types of equipment such as routers and switches.

The study of network topology recognizes eight basic topologies:

- Bus
- Point to point
- Star
- Ring or circular
- Mesh
- Tree
- Hybrid
- Daisy chain



DIFFERENT TYPES OF TOPOLOGIES

Unit – 3

Networking Technologies

Q.1 What is computer networking ?

Ans A computer network, often simply referred to as a network, is a collection of computers and other hardware components interconnected by communication channels that allow sharing of resources and information. Where at least one process in one device is able to send/receive data to/from at least one process residing in a remote device, then the two devices are said to be in a network. Simply, more than one computer interconnected through a communication medium for information interchange is called a computer network.

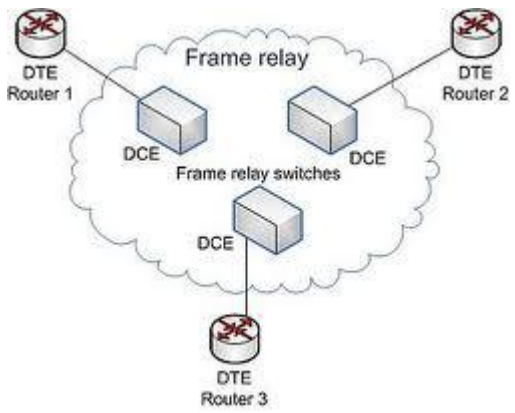
Networks may be classified according to a wide variety of characteristics, such as the medium used to transport the data, communications protocol used, scale, topology, and organizational scope.

Communications protocols define the rules and data formats for exchanging information in a computer network, and provide the basis for network programming. Well-known communications protocols include Ethernet, a hardware and link layer standard that is ubiquitous in local area networks, and the Internet protocol suite, which defines a set of protocols for internetworking, i.e. for data communication between multiple networks, as well as host-to-host data transfer, and application-specific data transmission formats.

Computer networking is sometimes considered a sub-discipline of electrical engineering, telecommunications, computer science, information technology or computer engineering, since it relies upon the theoretical and practical application of these disciplines.

Q.2 What is frame relay ?

Ans FRAM RELAY:--frame relay is a virtual circuit in wan that was designed in 1990.industry standard ,switched data link layer protocol that handles multiple virtual circuits between connected devices frame relay is more efficient than x.25the protocol for which is generally considered a replacement.



FRAME RELAY

- Frame relay operates at a high speed (recently 44.376mbps).
- Frame relay operates in physical and DLL. This means that it can be used as a back bone network.
- Frame relay allows a frame size of 9000bytes which can handles all local area network frame size.
- Frame relay has no error detection at the DLL or no error control .there is not even the retransmission facility a frame is damage or drop.
- Frame relay designed in this way to provide fast transmission data capability for more reliable media and for those protocol that have error control at the higher layer.

Q.3 What is asynchronous transmission mode ?

Ans Asynchronous transmission mode networking is the newst topology available at this time .unlike others it can carry both voice and data over network wire or fiber ATM transmits all packets as 53byte cells, that have a variety of identifires on them to determine such things as quality of service.

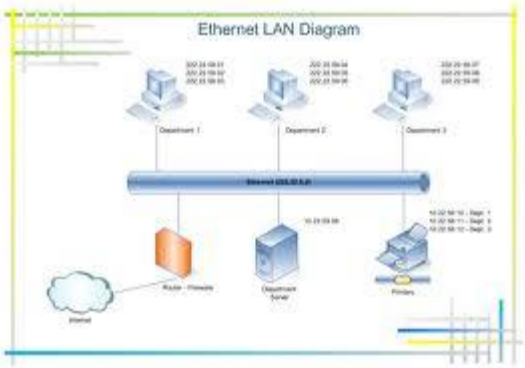
- Quality of service in packet data is similar to quality of sevice in regular mail. in regular mail you have a choice of service namely speed post air mail ect. when you send a speed post ,it receives priority over other types of mail so its gets to its destination first.

A few bits of data of data in a packet of data indicate the quality of services required for that data .when the quality of service feature is implemented you can send packet based on their need for band width

- ATM can provide for simultaneous data,video and voice transmission .it can be used for WAN,LAN and MAN. It can reach speeds of up to 2.488gigabits per second.

Q.4 What is Ethernet?

Ans ETHERNET:--Ethernet invented in 1973 by Bob Metcalf(who later formed a new company called 3 com, one of the most successful networking companies),was way to circumvent the limitation of earlier networks. It was based on an IEEE standard called 802.3CSMA/CD, and it provided for ways to manage the crazy situation that occurred when many computers tried to transmit on one wire simultaneously.



In terms of networking , collisn happiness when two computers attempt to transmit data on the same network wire at the same time .this creates a conflict both computers sense the collision ,stop transmitting ,and wait a random amount of time before retransmitting. Each computer can transmit data only when no other computer is currently transmitting .the larger the collision domain the more likely it is that collision will occur ,that is why ethernet designer try to keep the number of computers in a segment as low as possible.

Q.5 Explain the term fast Ethernet and gigabit Ethernet ?

Ans Gigabit Ethernet and Fast Ethernet :-- In computer networking , gigabit ethernet is a term describing various technologies for transmitting Ethernet frames at a rate of a gigabit per second (1,000,000,000 bits per second), as defined by the IEEE 802.3-2008 standard. It came into use beginning in 1999, gradually supplanting Fast Ethernet in wired local networks where it performed

considerably faster. The cables and equipment are very similar to previous standards, and by the year 2010, were very common and economical.

Half-duplex gigabit links connected through hubs are allowed by the specification, but full-duplex usage with switches is much more common.

There are five physical layer standards for gigabit Ethernet using optical fiber (1000BASE-X), twisted pair cable (1000BASE-T), or balanced copper cable (1000BASE-CX).

The IEEE 802.3z standard includes 1000BASE-SX for transmission over multi-mode fiber, 1000BASE-LX for transmission over single-mode fiber, and the nearly obsolete 1000BASE-CX for transmission over balanced copper cabling. These standards use 8b/10b encoding, which inflates the line rate by 25%, from 1000 Mbit/s to 1250 Mbit/s, to ensure a DC balanced signal. The symbols are then sent using NRZ.

IEEE 802.3ab, which defines the widely used 1000BASE-T interface type, uses a different encoding scheme in order to keep the symbol rate as low as possible, allowing transmission over twisted pair.

Q.6 What is ISDN ? explain.

Ans **I**ntegrated Services Digital Network (ISDN) is a set of communications standards for simultaneous digital transmission of voice, video, data, and other network services over the traditional circuits of the public switched telephone network. 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) 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. A major market application for ISDN in some countries is Internet access, where ISDN typically provides a maximum of 128 kbit/s in both upstream and downstream directions. Channel bonding can

achieve a greater data rate; typically the ISDN B-channels of 3 or 4 BRIs (6 to 8 64 kbit/s channels) are bonded.

ISDN should not be mistaken for its use with a specific protocol, such as Q.931 whereby ISDN is employed as the network, data-link and physical layers in the context of the OSI model. In a broad sense ISDN can be considered a suite of digital services existing on layers 1, 2, and 3 of the OSI model. ISDN is designed to provide access to voice and data services simultaneously.

However, common use reduced ISDN to be limited to Q.931 and related protocols, which are a set of protocols for establishing and breaking circuit switched connections, and for advanced calling features for the user. They were introduced in 1986.

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

Q.7 What is FDDI and CDDI ?explain

Ans Fiber Distributed Data Interface (FDDI) provides a 100 Mbit/s optical standard for data transmission in a local area network that can extend in range up to 200 kilometers (120 mi). Although FDDI logical topology is a ring-based token network, it does not use the IEEE 802.5 token ring protocol as its basis; instead, its protocol is derived from the IEEE 802.4 token bus timed token protocol. In addition to covering large geographical areas, FDDI local area networks can support thousands of users. As a standard underlying medium it uses optical fiber, although it can use copper cable, in which case it may be referred to as CDDI (Copper Distributed Data Interface). FDDI offers both a Dual-Attached Station (DAS), counter-rotating token ring topology and a Single-Attached Station (SAS), token bus passing ring topology.

FDDI was considered an attractive campus backbone technology in the early to mid 1990s since existing Ethernet networks only offered 10 Mbit/s transfer speeds and Token Ring networks only offered 4 Mbit/s or 16 Mbit/s speeds. Thus it was the preferred choice of that era for a high-speed backbone, but FDDI has since been effectively obsolesced by fast Ethernet which offered the same 100 Mbit/s speeds, but at a much lower cost and, since 1998, by Gigabit Ethernet due to its speed, and even lower cost, and ubiquity.

FDDI, as a product of American National Standards Institute X3T9.5 (now X3T12), conforms to the Open Systems Interconnection (OSI) model of functional layering of LANs using other protocols. FDDI-II, a version of FDDI, adds the

capability to add circuit-switched service to the network so that it can also handle voice and video signals. Work has started to connect FDDI networks to the developing Synchronou Optical Network (SONET).

A FDDI network contains two rings, one as a secondary backup in case the primary ring fails. The primary ring offers up to 100 Mbit/s capacity. When a network has no requirement for the secondary ring to do backup, it can also carry data, extending capacity to 200 Mbit/s. The single ring can extend the maximum distance; a dual ring can extend 100 km (62 mi). FDDI has a larger maximum-frame size (4,352 bytes) than standard 100 Mbit/s Ethernet which only supports a maximum-frame size of 1,500 bytes, allowing better throughput.

Designers normally construct FDDI rings in the form of a "dual ring of trees" (see network topology). A small number of devices (typically infrastructure devices such as routers and concentrators rather than host computers) connect to both rings - hence the term "dual-attached". Host computers then connect as single-attached devices to the routers or concentrators. The dual ring in its most degenerate form simply collapses into a single device. Typically, a computer-room contains the whole dual ring, although some implementations have deployed FDDI as a Metropolitan area network.

Qus8 What is SMDS ? explain.

Ans Switched Multi-megabit Data Service (SMDS) was a connectionless service used to connect LANs, MANs and WANs to exchange data, in early 1990s. In Europe, the service was known as Connectionless Broadband Data Service (CBDS).

SMDS was specified by Bellcore, and was based on the IEEE 802.6 metropolitan area network (MAN) standard, as implemented by Bellcore, and used cell relay transport, Distributed Queue Dual Bus layer-2 switching arbitrator, and standard SONET or G.703 as access interfaces.

Its a switching service that provides data transmission in the range between 1.544 Mbit/s (T1 or DS1) to 45 Mbit/s (T3 or DS3). SDMS was developed by Bellcore as an interim service until Asynchronous Transfer Mode matured. In the mid-1990s, SMDS was replaced, largely by Frame Relay.

SMDS was notable for its initial introduction of the 53-byte cell and cell switching approaches, as well as the method of inserting 53-byte cells onto G.703 and SONET.

Qus9 What is SONET ? explain.

Ans Synchronous Optical Networking (SONET) and Synchronous Digital Hierarchy (SDH) are standardized multiplexing protocols that transfer multiple digital bit streams over optical fiber using lasers or highly coherent light from light-emitting diodes (LEDs). At low transmission rates data can also be transferred via an electrical interface. The method was developed to replace the Plesiochronous Digital Hierarchy (PDH) system for transporting large amounts of telephone calls and data traffic over the same fiber without synchronization problems. SONET generic criteria are detailed in Telcordi Technologies Generic Requirements document GR-253-CORE. Generic criteria applicable to SONET and other transmission systems (e.g., asynchronous fiber optic systems or digital radio systems) are found in Telcordia GR-499-CORE.

SONET and SDH, which are essentially the same, were originally designed to transport circuit mode communications (e.g., DS1, DS3) from a variety of different sources, but they were primarily designed to support real-time, uncompressed, circuit-switched voice encoded in PCM format. The primary difficulty in doing this prior to SONET/SDH was that the synchronization sources of these various circuits were different. This meant that each circuit was actually operating at a slightly different rate and with different phase. SONET/SDH allowed for the simultaneous transport of many different circuits of differing origin within a single framing protocol. SONET/SDH is not itself a communications protocol per se, but a transport protocol.

Due to SONET/SDH's essential protocol neutrality and transport-oriented features, SONET/SDH was the obvious choice for transporting the fixed length Asynchronous Transfer Mode (ATM) frames also known as cells. It quickly evolved mapping structures and concatenated payload containers to transport ATM connections. In other words, for ATM (and eventually other protocols such as Ethernet), the internal complex structure previously used to transport circuit-oriented connections was removed and replaced with a large and concatenated frame (such as OC-3c) into which ATM cells, IP packets, or Ethernet frames are placed.

Racks of Alcatel STM-16 SDH add-drop multiplexers

Both SDH and SONET are widely used today: SONET in the United States and Canada, and SDH in the rest of the world. Although the SONET standards were developed before SDH, it is considered a variation of SDH because of SDH's greater worldwide market penetration.

The SDH standard was originally defined by the European Telecommunications Standards Institute (ETSI), and is formalized as International Telecommunication Union (ITU) standards G.707, G.783, G.784,and G.803.The SONET standard was defined by Telcordia and American National Standards Institute(ANSI) standard T1.105.

Q.10 What is DWDM ? explain.

Ans DWDM (Dense Wavelength devision Multiplexing):-- it refers originally to optical signals multiplexed within the 1550 nm band so as to leverage the capabilities (and cost) of erbium doped fiber amplifiers (EDFAs), which are effective for wavelengths between approximately 1525–1565 nm (C band), or 1570–1610 nm (L band). EDFAs were originally developed to replace SONET/SDH optical-electrical-optical (OEO) regenerators, which they have made practically obsolete. EDFAs can amplify any optical signal in their operating range, regardless of the modulated bit rate.

DWDM Systems :- At this stage, a basic DWDM system contains several main components:

1. A DWDM terminal multiplexer. The terminal multiplexer actually contains one wavelength converting transponder for each wavelength signal it will carry. The wavelength converting transponders receive the input optical signal (i.e., from a client-layer SONET/SDH or other signal), convert that signal into the electrical domain, and retransmit the signal using a 1550 nm band laser. (Early DWDM systems contained 4 or 8 wavelength converting transponders in the mid 1990s. By 2000 or so, commercial systems capable of carrying 128 signals were available.) The terminal mux also contains an optical multiplexer, which takes the various 1550 nm band signals and places them onto a single fiber (e.g. SMF-28 fiber). The terminal multiplexer may or may not also support a local EDFA for power amplification of the multi-wavelength optical signal.
2. An intermediate line repeater is placed approx. every 80 – 100 km for compensating the loss in optical power, while the signal travels along the fiber. The signal is amplified by an EDFA, which usually consists of several amplifier stages.
3. An intermediate optical terminal, or optical add-drop multiplexer. This is a remote amplification site that amplifies the multi-wavelength signal that may have traversed up to 140 km or more before reaching the remote site. Optical diagnostics and telemetry are often extracted or inserted at such a site, to allow for localization of any fiber breaks or signal impairments. In more sophisticated

systems (which are no longer point-to-point), several signals out of the multiwavelength signal may be removed and dropped locally.

4. A DWDM terminal demultiplexer. The terminal demultiplexer breaks the multi-wavelength signal back into individual signals and outputs them on separate fibers for client-layer systems (such as SONET/SDH) to detect. Originally, this demultiplexing was performed entirely passively, except for some telemetry, as most SONET systems can receive 1550-nm signals. However, in order to allow for transmission to remote client-layer systems (and to allow for digital domain signal integrity determination) such demultiplexed signals are usually sent to O/E/O output transponders prior to being relayed to their client-layer systems. Often, the functionality of output transponder has been integrated into that of input transponder, so that most commercial systems have transponders that support bi-directional interfaces on both their 1550-nm (i.e., internal) side, and external (i.e., client-facing) side. Transponders in some systems supporting 40 GHz nominal operation may also perform forward error correction (FEC) via 'digital wrapper' technology, as described in the ITU-T G.709 standard.
5. Optical Supervisory Channel (OSC). This is an additional wavelength usually outside the EDFA amplification band (at 1510 nm, 1620 nm, 1310 nm or another proprietary wavelength). The OSC carries information about the multi-wavelength optical signal as well as remote conditions at the optical terminal or EDFA site. It is also normally used for remote software upgrades and user (i.e., network operator) Network Management information. It is the multi-wavelength analogue to SONET's DCC (or supervisory channel). ITU standards suggest that the OSC should utilize an OC-3 signal structure, though some vendors have opted to use 100 megabit Ethernet or another signal format. Unlike the 1550 nm band client signal-carrying wavelengths, the OSC is always terminated at intermediate amplifier sites, where it receives local information before retransmission.

Unit – 4

Network Switching

Q.1 What is switching ?

Ans **S**witches are hardware or software devices capable of creating temporary connection between two or more devices link.link to the switch but not to each other .

There are three methods of switching :-

(1) circuit switching

(2) message switching

(3) packet switching

Q.2 What is circuit switching ?

Ans Circuit switching creates a direct physical connection between two devices such as phone .in this transmission line is open between two parties until their communication is finished circuit switching is efficient for connection that carry a large amount of data.

Circuit switching is appropriate for voice data .it is a method of networking in which communicating machines have exclusive view of the circuit linking the, even during passes, when the circuit is idel.

Q.3 What is message switching ?

Ans **I**n a message switching the central switch station accepts the traffic sent to it by the station connected to it.

The message are stored in the switch stations buffer memory and a line is available, Tthe data are forwarded to the appropriate station. Thus the message switching is also known as stored and forward method.

The benefit whit message switching is that when the sending station has finished sending .it's traffic, it can send data to another.

Q.4 What is packet switching ?

Ans **P**acket switching is an allocation technique that uses bandwidth only when there is data to be transmitted the packet header identifies the source of the data and destination and it can also identify the nature of data.
The problem with message switching is the main difficulty with implementing system using message switching is the need to allocate the large data buffer to hold incoming message and the time it takes for a message to reach its destination complicated software programs are required to manage the routing and storage of these messages.

Long messages are broken into smaller units in packet switching and the units are called "packet".

Q.5 What is virtual LAN ?

Ans. VIRTUAL LAN is a networking technology that allows networks to be segmented logically without having to be physically rewired.
Rationally each department in a building used to have its own local area network .these LAN were created using hubs and these hubs were connected to a main Ethernet switch in the main room of the building .how ever broadcast sent by any hosts on the network ,even if all the hosts do not need to receive them. Also, if the location of the department changes, the hubs must be rewired to reflect the new topology of the network.
To overcome these problems, many Ethernet switches nowadays

Support virtual LAN (VLAN) technologies .all hubs are replaced by van switches the network administrator creates virtual network segments whose logical topology is independent of the physical topology of the wiring. Each station is assigned a VLAN identification number (id) ,and station with the same VLAN ID can act and function as though they are all on the same physical network segment.

Broadcast sent by one host are received only by hosts with the same VLAN ID. The assignment if VLAN ID is done at the port level on the switches themselves and can be managed remotely using network management software.

Advantage of VLAN: the main advantage of using VLAN technologies is that users can be grouped together according to their need for network communication, regardless of their actual physical location.

Disadvantage of VLAN: the only disadvantage is that additional equipment is required to set up and establish the VLANs.

Q.6 Explain non ATM?

Ans. Asynchronous Transfer Mode (ATM) is, according to the ATM Forum, "a telecommunications concept defined by ANSI and ITU (formally CCITT) standards for carriage of a complete range of user traffic, including voice, data, and video signals, "and is designed to unify telecommunication and computer networks. It uses asynchronous time-division multiplexing, and it encodes data into small, fixed-sized cells. This differs from approaches such as the Internet Protocol or Ethernet that use variable sized packets or frames. ATM provides data link layer services that run over a wide range of OSI physical Layer links. ATM has functional similarity with both circuit switched networking and small packet switched networking. It was designed for a network that must handle both traditional high-throughput data traffic (e.g., file transfers), and real-time, low-latency content such as voice and video. ATM uses a connection-oriented model in which a virtual circuit must be established between two endpoints before the actual data exchange begins. ATM is a core protocol used over the SONET/SDH backbone of the public switched telephone network (PSTN) and Integrated Services Digital Network (ISDN), but its use is declining in favor of All IP

.

Q.7 What is IEEE802.1Q VLAN standards?

Ans. IEEE 802.1Q is the networking standard that supports Virtual LANs (VLANs) on an Ethernet network. The standard defines a system of VLAN tagging for Ethernet frames and the accompanying procedures to be used by bridges and switches in handling such frames. The standard also contains provisions for a quality of service prioritization scheme commonly known as IEEE 802.1p and defines the Generic Attribute Registration Protocol.

Portions of the network which are VLAN-aware (i.e., IEEE 802.1Q conformant) can include VLAN tags. Traffic on a VLAN-unaware (i.e., IEEE 802.1D conformant) portion of the network will not contain VLAN tags. When a frame enters the VLAN-aware portion of the network, a tag is added to represent the VLAN membership of the frame's port or the port/protocol combination, depending on whether port-based or port-and-protocol-based VLAN classification is being used. Each frame must be distinguishable as being within exactly one VLAN. A frame in the VLAN-aware portion of the network that does

not contain a VLAN tag is assumed to be flowing on the native (or default) VLAN.

The standard was developed by IEEE 802.1, a working group of the IEEE 802 standards committee and continues to be actively revised with notable revisions including IEEE 802.1ak, IEEE 802.1Qat and IEEE 802.1Qay.

Q.8 what is simulation?

Ans. In computer science, simulation has some specialized meanings: Alan Turing used the term "simulation" to refer to what happens when a universal machine executes a state transition table (in modern terminology, a computer runs a program) that describes the state transitions, inputs and outputs of a subject discrete-state machine. The computer simulates the subject machine. Accordingly, in theoretical computer science the term *simulation* is a relation between state transition systems, useful in the study of operational semantics.

Less theoretically, an interesting application of computer simulation is to simulate computers using computers. In computer architecture, a type of simulator, typically called an *emulator*, is often used to execute a program that has to run on some inconvenient type of computer (for example, a newly designed computer that has not yet been built or an obsolete computer that is no longer available), or in a tightly controlled testing environment (see *Computer architecture simulator* and *Platform virtualization*). For example, simulators have been used to debug a micro program or sometimes commercial application programs, before the program is downloaded to the target machine. Since the operation of the computer is simulated, all of the information about the computer's operation is directly available to the programmer, and the speed and execution of the simulation can be varied at will.

Simulators may also be used to interpret fault trees, or test VLSI logic designs before they are constructed. Symbolic simulation uses variables to stand for unknown values.

In the field of optimization, simulations of physical processes are often used in conjunction with evolutionary computation to optimize control strategies.

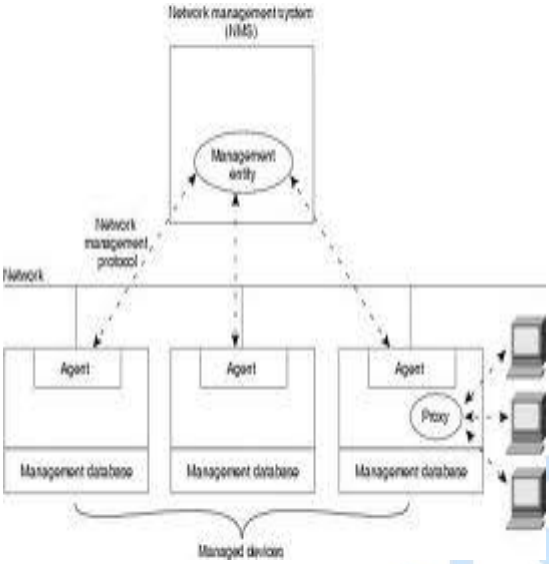
Unit– 5

Network Management

Q.1 What is network management?

Ans. Network management refers to the activities, methods, procedures, and tools that pertain to the operation, administration, maintenance, and provisioning of networked systems.

- Operation deals with keeping the network (and the services that the network provides) up and running smoothly. It includes monitoring the network to spot problems as soon as possible, ideally before users are affected.
- Administration deals with keeping track of resources in the network and how they are assigned. It includes all the "housekeeping" that is necessary to keep the network under control.
- Maintenance is concerned with performing repairs and upgrades—for example, when equipment must be replaced, when a router needs a patch for an operating system image, when a new switch is added to a network. Maintenance also involves corrective and preventive measures to make the managed network run "better", such as adjusting device configuration parameters.
- Provisioning is concerned with configuring resources in the network to support a given service. For example, this might include setting up the network so that a new customer can receive voice service.



NETWORK MANAGEMENT

Functions that are performed as part of network management accordingly include controlling, planning, allocating, deploying, coordinating, and monitoring the resources of a network, network planning, frequency allocation, predetermined traffic routing to support load balancing, cryptographic key distribution authorization, configuration management, fault management, security management, performance management, bandwidth management, Route analytics and accounting management.

Q.2 What is directory services?

Ans. A directory service is the software system that stores, organizes and provides access to information in a directory. In software engineering, a directory is a map between names and values. It allows the lookup of values given a name, similar to a dictionary. As a word in a dictionary may have multiple definitions, in a directory, a name may be associated with multiple, different pieces of information. Likewise, as a word may have different parts of speech and different definitions, a name in a directory may have many different types of data.

Directories may be very narrow in scope, supporting only a small set of node types and data types, or they may be very broad, supporting an arbitrary or extensible set of types. In a telephone directory, the nodes are names and the data items are telephone numbers. In the DNS the nodes are domain names and the data items are IP addresses (and alias, mail server names, etc.). In a directory

used by a network operating system, the nodes represent resources that are managed by the OS, including users, computers, printers and other shared resources. Many different directory services have been used since the advent of the Internet but this article focuses mainly on those that have descended from the X.500 directory service.

Q.3 What is SNMP?

Ans. SNMP it stands for simple network management protocol .SNMP is an internet standard application layer (layer 7) protocol for exchanging device management information between network devices on a TCP/IP network .simple network management protocol (SNMP)is most often used for collecting statically and configuration information about network devices such as computer ,hubs,switches,routers and even network printers. the statistical information includes the number of packets or frames sent or received per second the number of error per second etc.the configuration information include the IP address of an interface on the device, the version of the operating system running of the device etc. management systems are used to monitor network health, trap errors perform diagnostic and generate reports .SNMP is the most popular network management protocol in use.

Q.4 Explain the network management technology?

Ans. A small number of accessories methods exist to support network and network device management. Access methods include the SNMP, command-line interface (CLIs), custom XML, CMIP, Windows Management Instrumentation (WMI), Transaction Language 1, CORBA, NETCONF, and the Java Management Extensions (JMX). Internet service providers (ISP) use a technology known as deep packet inspection in order to regulate network congestion and lessen Internet bottlenecks.

Schemas include the WBEM, the Common Information Model, and MTOSI amongst others.

Medical Service Providers provide a niche marketing utility for managed service providers; as HIPAA legislation consistently increases demands for knowledgeable providers. Medical Service Providers are liable for the protection of their client's confidential information, including in an electronic realm. This liability creates a significant need for managed service providers who can provide secure infrastructure for transportation of medical data.

Q.5 What is TMN?

Ans. The Telecommunications Management Network is a protocol model defined by ITU-T for managing open systems in a communications network. It is part of the ITU-T Recommendation series M.3000 and is based on the OSI management specifications in ITU-T Recommendation series X.700.

TMN provides a framework for achieving interconnectivity and communication across heterogeneous operations system and telecommunication networks. To achieve this, TMN defines a set of *interface points* for elements which perform the actual communications processing (such as a call processing switch) to be accessed by elements, such as management workstations, to monitor and control them. The standard interface allows elements from different manufacturers to be incorporated into a network under a single management control.

For communication between Operations Systems and NEs (Network Elements), it uses the Common management information protocol (CMIP) or Mediation devices when it uses Q3 interface.

TMN can be used in the management of ISDN, B-ISDN, ATM, and GSM networks. It is not as commonly used for purely packet-switched data networks.

Modern telecom networks are automated, and are run by OSS software or operational support systems. These manage modern telecom networks and provide the data that is needed in the day-to-day running of a telecom network. OSS software is also responsible for issuing commands to the network infrastructure to activate new service offerings, commence services for new customers, and detect and correct network faults.

Q.6 Explain RMON?

Ans. The Remote Network Monitoring (RMON) MIB was developed by the IETF to support monitoring and protocol analysis of LANs. The original version (sometimes referred to as RMON1) focused on OSI Layer 1 and Layer 2 information in Ethernet and Token Ring networks. It has been extended by RMON2 which adds support for Network- and Application-layer monitoring and by SMON which adds support for switched networks. It is an industry standard specification that provides much of the functionality offered by

proprietary network analyzers. RMON agents are built into many high-end switches and routers.

An RMON implementation typically operates in a client/server model. Monitoring devices (commonly called "probes" in this context) contain RMON software agents that collect information and analyze packets. These probes act as servers and the Network Management applications that communicate with them act as clients. While both agent configuration and data collection use SNMP, RMON is designed to operate differently than other SNMP-based systems:

- Probes have more responsibility for data collection and processing, which reduces SNMP traffic and the processing load of the clients.
- Information is only transmitted to the management application when required, instead of continuous polling.

In short, RMON is designed for "flow-based" monitoring, while SNMP is often used for "device-based" management. RMON is similar to other flow-based monitoring technologies such as Net Flow and Slow because the data collected deals mainly with traffic patterns rather than the status of individual devices. One disadvantage of this system is that remote devices shoulder more of the management burden, and require more resources to do so. Some devices balance this trade-off by implementing only a subset of the RMON MIB groups (see below). A minimal RMON agent implementation could support only statistics, history, alarm, and event

Unit – 6

Network Security

Q.1 Explain network performance?

Ans. Network performance refers to the service quality of a telecommunications product as seen by the customer. It should not be seen merely as an attempt to get "more through" the network.

The following list gives examples of Network Performance measures for a circuit-switched network and one type of packet-switched network, viz. ATM:

- **Circuit-switched networks**: In circuit switched networks, network performance is synonymous with the grade of service. The number of rejected calls is a measure of how well the network is performing under heavy traffic loads. Other types of performance measures can include noise, echo and so on.
- **ATM**: In an Asynchronous Transfer Mode (ATM) network, performance can be measured by line rate, quality of service(QoS), data throughput, connect time, stability, technology, modulation technique and modem enhancements.

There are many different ways to measure the performance of a network, as each network is different in nature and design. Performance can also be modeled instead of measured; one example of this is using state transition diagrams to model queuing performance in a circuit-switched network. These diagrams allow the network planner to analyze how the network will perform in each state, ensuring that the network will be optimally designed.

Q.2 What is network security? Explain.

Ans. Due to the wide space use of PCs and developments in networks connecting PCs to companies main frame computers, there has been an increase in the chances of feeding undesirable data deliberately by outsiders. A person with a PC at a remote place can use a phone line and illegally collect information without leaving any clues. Individual users can copy confidential data from a company's computer or other details from a remote station connected via a communication network.

"The collection of tools designed to protect data and thwart hackers is known as computer security".

Security means preventing the network communication system falling in the hands of unauthorized people. The sender of data must be assured that only the intended party actually receives designated data.

The network security methods adopted must address the following issues:--

(a) Information in a computer system should only be accessed by authorized persons.

(b) The shareable resources must be available only for use by authorized members.

(c) Unauthorized person should not be able to insert spurious messages or records into a file being transmitted in a network.

(d) It should not be possible for an unauthorized party to perform wiretapping in order to capture the data or illicitly copy files and /or programs.

Q.3 Explain the security management?

Ans. Security Management:--guidelines for deciding on the security and management are the following:

(a) What level of security management is really required?

(b) What level of management should be developed? Typically, performance and fault management is deployed .one can also deploy accounting ,configuration and security management depending on the requirements

(c) Physical security of the networks, devices etc, is also to be kept in mind.

(d) Security policies should be modified continuously depending on the threat perception from virus or external sources.

(e) One old truism in security is that the cost of protecting yourself against the threat should be less than the cost of recovering if the threat were to strike you .cost in this context should include the losses expected expressed in real currency, reputation, trustworthiness, and other less obvious manner (as referred in RFC2196)

Once we complete this analysis, we are ready with the logical network for the requirements. This helps to make the network design more robust and brings it closer to achieving the goals set by the client.

Q.4 What is VPN? Explain.

Ans. VPN (virtual private network):--VPN is a private network of an organization built over a public network such as the internet .thus the connections protocols and services used in VPN are those of public networks, but it is so built that it would function as a private corporate network.

For companies, VPN are very cost effective than a network provided by using modems, dedicated leased lines and toll free numbers.

In vans users enjoy the same security and privacy features as available in a real private network .it gives secure remote access to the corporate network over the internet.

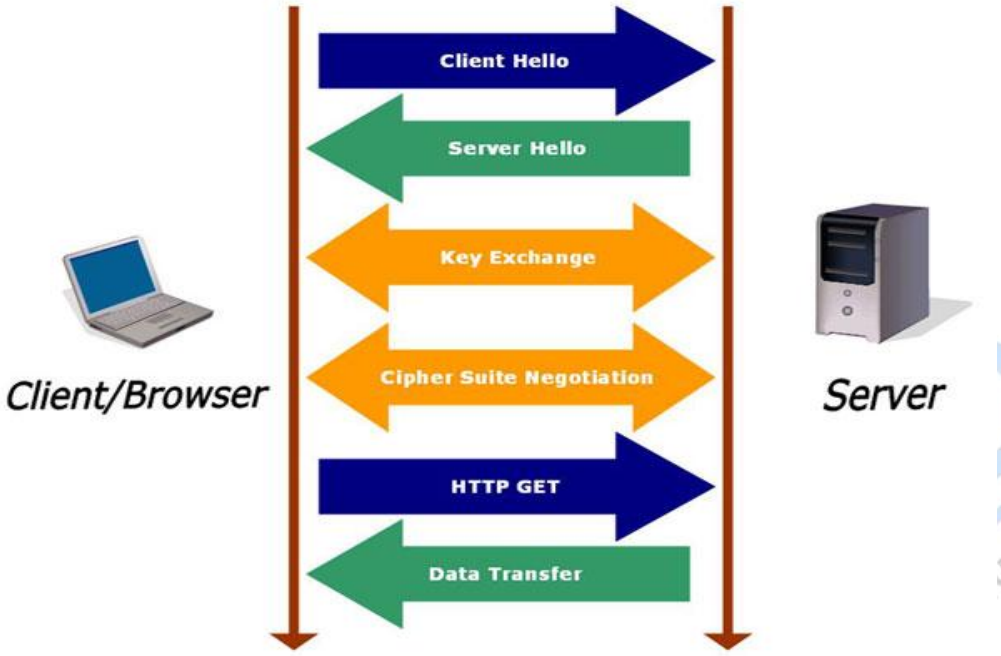
The internet service provider (isp)can install a remote authentication dial in user services (RADIUS)proxy server and configure it to recognize and authenticate request from the employees of the company using VPN, and forward it to the IAS(internet authentication service)on the company's private network. In this way, the VPN customer would be able to keep control over the remote access permissions for all its employees

VPNs use tunneling technologies to allow users to access private network resources through the internet or any other public network.

Q.5 What is SSL?

Ans. **SSL**:-- Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL), are cryptographic protocols that provide communication security over the Internet.TLS and SSL encrypt the segments of network connections at the Application Layer for the Transport Layer, using asymmetric cryptography for key exchange, symmetric encryption for privacy, and message authentication codes for message integrity.

Several versions of the protocols are in widespread use in applications such as web browsing, electronic mail, Internet faxing, instant messaging and voice-over-IP (VoIP).



The TLS protocol allows client-server applications to communicate across a network in a way designed to prevent eavesdropping and tampering.

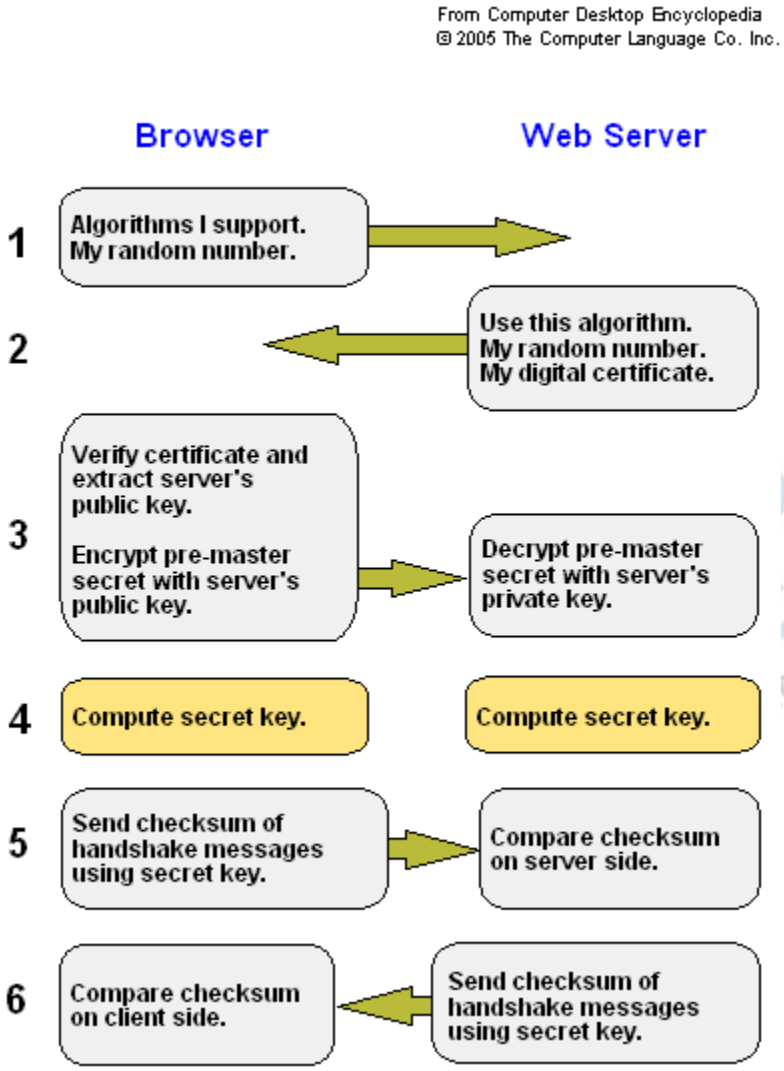
Since most protocols can be used either with or without TLS (or SSL) it is necessary to indicate to the server whether the client is making a TLS connection or not. There are two main ways of achieving this; one option is to use a different port number for TLS connections (for example port 443 for HTTPS).

Once the client and server have decided to use TLS they negotiate a crateful connection by using a handshaking procedure. During this handshake, the client and server agree on various parameters used to establish the connection's security.

1. The client sends the server the client's SSL version number, cipher settings, session-specific data, and other information that the server needs to communicate with the client using SSL.
2. The server sends the client the server's SSL version number, cipher settings, session-specific data, and other information that the client needs to communicate with the server over SSL. The server also sends its own certificate, and if the client is requesting a server resource that requires client authentication, the server requests the client's certificate.
3. The client uses the information sent by the server to authenticate the server (see Server Authentication for details). If the server cannot be authenticated,

the user is warned of the problem and informed that an encrypted and authenticated connection cannot be established. If the server can be successfully authenticated, the client proceeds to step 4.

4. Using all data generated in the handshake thus far, the client (with the cooperation of the server, depending on the cipher being used) creates the pre-master secret for the session, encrypts it with the server's public key (obtained from the server's certificate, sent in step 2), and then sends the encrypted pre-master secret to the server.
5. If the server has requested client authentication (an optional step in the handshake), the client also signs another piece of data that is unique to this handshake and known by both the client and server. In this case, the client sends both the signed data and the client's own certificate to the server along with the encrypted pre-master secret.
6. If the server has requested client authentication, the server attempts to authenticate the client (see Client Authentication for details). If the client cannot be authenticated, the session ends. If the client can be successfully authenticated, the server uses its private key to decrypt the pre-master secret, and then performs a series of steps (which the client also performs, starting from the same pre-master secret) to generate the master secret.
7. Both the client and the server use the master secret to generate the session keys, which are symmetric keys used to encrypt and decrypt information exchanged during the SSL session and to verify its integrity (that is, to detect any changes in the data between the time it was sent and the time it is received over the SSL connection).
8. The client sends a message to the server informing it that future messages from the client will be encrypted with the session key. It then sends a separate (encrypted) message indicating that the client portion of the handshake is finished.
9. The server sends a message to the client informing it that future messages from the server will be encrypted with the session key. It then sends a separate (encrypted) message indicating that the server portion of the handshake is finished.



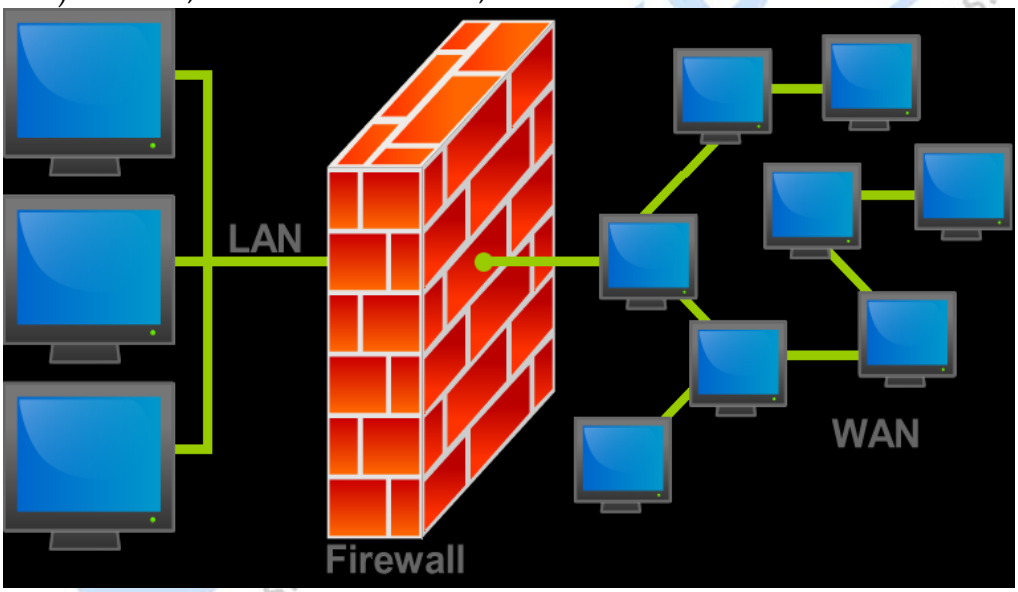
The SSL handshake is now complete and the session begins. The client and the server use the session keys to encrypt and decrypt the data they send to each other and to validate its integrity.

This is the normal operation condition of the secure channel. At any time, due to internal or external stimulus (either automation or user intervention), either side may renegotiate the connection, in which case, the process repeats itself.

Q.6 Explain firewalls?

Ans. FIREWALL:--firewalls are hardware and software combination that are built using routers, servers and a variety of software .they sit at the most vulnerable point between a corporate network and the internet and they can be as simple or complex as system administrators want to build them. Firewalls reduce the speed of access to networks.

A firewall can either be software-based or hardware-based and is used to help keep a network secure. Its primary objective is to control the incoming and outgoing network traffic by analyzing the data packets and determining whether it should be allowed through or not, based on a predetermined rule set. A network's firewall builds a bridge between an internal network that is assumed to be secure and trusted, and another network, usually an external (inter)network, such as the Internet, that is not assumed to be secure and trusted.



Many personal computer operating systems include software-based firewalls to protect against threats from the public Internet. Many routers that pass data between networks contain firewall components and, conversely, many firewalls can perform basic routing functions.

Q.7 What is Kerberos?

Ans. **Kerberos**:--is a computer network authentication protocol which works on the basis of "tickets" to allow nodes communicating over a non-secure network to prove their identity to one another in a secure manner. Its designers aimed primarily at a client–server model, and it provides mutual authentication-both

the user and the server verify each other's identity. Kerberos protocol messages are protected against eavesdropping and replay attacks. Kerberos builds on symmetric key cryptography and requires a trusted third party, and optionally may use public-key cryptography by utilizing asymmetric key cryptography during certain phases of authentication. Kerberos uses port 88 by default.

"Kerberos" also refers to a suite of free software published by Massachusetts Institute of Technology (MIT) that implements the Kerberos protocol.

Q.8 Write short note on cyber laws?

Ans. **I**n simple language we can say that the meaning of cyber laws is unlawful acts wherein the computer is either a tool or a target or both now we can understand the meaning of cyber crime .cyber law is term that encapsulates the legal issues of the internet it is the less distinct field of law than contract law ,as it is a domain converting many areas of law and then regulation .the internet defies geographical boundaries ,national laws can not apply globally and it has been suggested instead that the internet can be self regulated as being its own transnational .

Cyber law is a term that encapsulates the legal issues related to use of the internet .it is the less distinct field of law than intellectual property or contract law, as it is a domain covering many areas of law and regulation. Some Topics: - internet access and usage, privacy, freedom of expression, and jurisdiction.

Multiple Choice Questions

1. The _____ is the physical path over which a message travels.
    1. Protocol
    2. Medium
    3. Signal
    4. All the above

2. The information to be communicated in a data communications system is the _____.
    1. Medium
    2. Protocol
    3. **Message**
    4. Transmission

3. Frequency of failure and network recovery time after a failure are measures of the _____of a network.
    1. Performance
    2. Reliability
    3. Security
    4. Feasibility

4. An unauthorized user is a network _____ issue.
    1. Performance
    2. Reliability
    3. **Security**
    4. All the above

5. Which topology requires a central controller or hub?
    1. Mesh
    2. **Star**
    3. Bus
    4. Ring

6. Which topology requires a multipoint connection?
    1. Mesh

2. Star
3. Bus
4. Ring

7. Communication between a computer and a keyboard involves _____ transmission.
1. **Simplex**
2. half-duplex
3. full-duplex
4. Automatic

8. A television broadcast is an example of _____ transmission.
1. **Simplex**
2. Half-duplex
3. full-duplex
4. Automatic

9. A _____ connection provides a dedicated link between two devices.
1. **Point-to-point**
2. Multipoint
3. Primary
4. Secondary

10. In a _____ connection, more than two devices can share a single link.
1. Point-to-point
2. **Multipoint**
3. Primary
4. Secondary

11. In _____ transmission, the channel capacity is shared by both communicating devices at all times.
1. Simplex
2. half-duplex
3. **full-duplex**
4. half-simplex

12. In the original ARPANET, _____ were directly connected together.

1. **IMPs**
2. Host computers
3. Networks
4. Routers

13. This was the first network.

A) CSNET
B) NSFNET
C) ANSNET
D) **ARPANET**

14. Which organization has authority over interstate and international commerce in the communications field?

1. ITU-T
2. IEEE
3. **FCC**
4. ISOC

15. _____ are special-interest groups that quickly test, evaluate, and standardize new technologies.

1. **Forums**
2. Regulatory agencies
3. Standards organizations
4. All of the above

16. Which agency developed standards for physical connection interfaces and electronic signaling specifications?

1. **EIA**
2. ITU-T
3. ANSI
4. ISO

17. _____ is the protocol suite for the current Internet.

1. **TCP/IP**
2. NCP
3. UNIX
4. ACM

18. _____ refers to the structure or format of the data, meaning the order in which they are presented.
1. Semantics
2. **Syntax**
3. Timing
4. All of the above

19. _____ defines how a particular pattern to be interpreted, and what action is to be taken based on that interpretation.
1. **Semantics**
2. Syntax
3. Timing
4. None of the above

20. _____ refers to two characteristics: when data should be sent and how fast it can be sent.
1. Semantics
2. Syntax
3. **Timing**
4. None of the above

21. Data flow between two devices can occur in a _____ way.
1. Simplex
2. half-duplex
3. full-duplex
4. **All of the above**

22. In a _____ connection, two and only two devices are connected by a dedicated link.
1. Multipoint
2. **Point-to-point**
3. (1) and (2)
4. None of the above

23. In a _____ connection, three or more devices share a link.
A) **multipoint**
B) point-to-point

C) (a) and (b)
4. None of the above

24. _____ refers to the physical or logical arrangement of a network.
A) Data flow
B) Mode of operation
C) **Topology**
D) None of the above

25. Devices may be arranged in a _____ topology.
1. Mesh
2. Ring
3. Bus
4. **All of the above**

26. A _____ is a data communication system within a building, plant, or campus, or between nearby buildings.
1. MAN
2. **LAN**
3. WAN
4. None of the above

27. A _____ is a data communication system spanning states, countries, or the whole world.
1. MAN
2. LAN
3. **WAN**
4. None of the above

28. _____ is a collection of many separate networks.
1. A WAN
2. **An internet**
3. A LAN
4. None of the above

29. There are _____ Internet service providers.
1. Local

2. Regional
3. National and international
4. **All of the above**

30. A _____ is a set of rules that governs data communication.
1. Forum
2. **Protocol**
3. Standard
4. None of the above

31. _____ is an idea or concept that is a precursor to an Internet standard.
1. RCF
2. **RFC**
3. ID
4. None of the above

32. If a computer on the network shares resources for others to use, it is called ____
1**. Server**
2. Client
3. Mainframe

33. Terminators are used in _____ topology**.**
1. **Bus**
2. Star

34. In _____ topology, if a computer's network cable is broken, whole network goes down.
1. **Bus**
2. Star

35. For large networks, _____ topology is used**.**
1. Bus
2. **Star**
3. Ring

36. ISO stands for
   1. **International Standard Organization**
2. International Student Organization
3. Integrated Services Organization

37. ISO OSI model is used in
   1. Stand alone PC
   2. **Network environment**

38. ____ Layer decides which physical pathway the data should take.
   1. Application
   2. Network
   3. **Physical**

39. ISDN is an example of _____ network
   1. **Circuit switched**
   2. Packet switched

40. X.25 is an example of _____ network
   1. Circuit switched
   2. **Packet switched**

41. _____ allows LAN users to share computer programs and data.
   1. Communication server
   2. Print server
   3. **File server**

42. Print server uses _____ which is a buffer that holds data before it is send to the printer.
   1. Queue
   2. **Spool**
   3. Node

43. A standalone program that has been modified to work on a LAN by including concurrency controls such as file and record locking is an example of____
   1. **LAN intrinsic software**

2. LAN aware software
3. Groupware
4. LAN ignorant software

44. The _____ portion of LAN management software restricts access, records user activities and audit data etc.
1. Configuration management
2. **Security management**
3. Performance management

45. What is the max cable length of STP?
1. 100 ft
2. 200 ft
3. 100 m
4. **200 m**

46. What is the max data capacity of STP?
1. 10 mbps
2. **100 mbps**
3. 1000 mbps
4. 10000 mbps

47. Which connector STP uses?
1. BNC
2. RJ-11
3. **RJ-45**
4. RJ-69

48. What is the central device in star topology?
1. STP server
2. **Hub/switch**
3. PDC
4. Router

49. What is max data capacity for optical fiber cable?
1. 10 mbps
2. 100 mbps

3. **1000 mbps**
4. 10000 mbps

50. Which of the following architecture uses CSMA/CD access method?
1. ARC net
2. **Ethernet**

51. A remote batch-processing operation in which data is solely input to a central computer would require
1. Telegraph line
2. **Simplex lines**
3. Mixed bad channel
4. All of above

52. A band is always equivalent to
1. A byte
2. A bit
3. 100 bits
4. **None of above**

53. The loss in signal power as light travels down the fiber is called
1. **Attenuation**
2. Prorogation
3. Scattering
4. Interruption

54. Avalanche photodiode receivers can detect bits of transmitted data by receiving
1. 100 photons
2. **200 photons**
3. 2000 photons
4. 300 photons

55. Communication circuits that transmit data in both directions but not at the same time are operating in
1. A simplex mode
2. **A half duplex mode**
3. A full duplex mode

4. An asynchronous mode

56. An example of a medium speed, switched communications service is
1. Series 1000
2. Data phone 50
3. **DDD**
4. All of the above

57. In communication satellite, multiple repeaters are known as
1. Detector
2. Modulator
3. Stations
4. **Transponders**

58. While transmitting odd-parity coded symbols, the number of zeros in each symbol is
1. Odd
2. Even
3. 1 and 2 both
4. **Unknown**

59. Data communications monitors available on the software marked include
1. **ENVIRON/1**
2. TOTAL
3. BPL
4. Telnet

60. An example of an analog communication method is
1. Laser beam
2. Microwave
3. Voice grade telephone line
4. **All of the above**

61. Bridges can not be the solution to
1. Limited distance
2. Limited traffic
3. Limited number of stations
4. **Packet redundancy**

62. The event that will not cause recalculation of the distance vector is
    1. Discovery of a long path to a new destination
    2. Discovery that a link to a neighbor has gone down
    3. Receive a shorter path to an existing destination
    4. **Discovery of a longer path to an existing destination**

63. BOOTP is a possible solution to the problem
    1. **Host IP address must be changed if he moves from one network to another**
    2. The limited address space
    3. All hosts addresses must be changed if class B networks grow too large
    4. All hosts addresses must be changed at least once a year

64. Which one of the media types is Multi - Drop?
    1. Unshielded Twisted Pairs
    2. **Thick Coaxial cable**
    3. Fiber Optic cable
    4. Shielded Twisted Pairs

65. While routing
    1. **Destination physical address changes every hop**
    2. Destination physical and IP addresses changes every hop
    3. Source IP address changes every hop
    4. Destination IP address changes every hop

66. ICMP
    1. **Messages are encapsulated in an IP header**
    2. Reports only on errors and problems
    3. Is integral part of TCP
    4. Is integral part of UDP

67. Domain Name System
    1. Tries to resolve names with root name servers first
    2. **Can be used in local environments**
    3. Provides mapping from Human-readable names to MAC addresses
    4. Each root name server who can? resolve the name sends the request to the hierarchically upper server

68. Which of the following is not provided by DHCP?
    1. IP address
    2. **ARP tables**
    3. Subnet mask
    4. DNS server address

69. RIP was popular because
    1. Intended for use on large, long-haul networks
    2. Has unbounded number of hops
    3. **It was distributed with Berkeley UNIX**
    4. RFC finally appeared in 1998

70. RIP
    1. Requires more memory than OSPF
    2. Provides load balancing
    3. Is implemented less than OSPF
    4. **Has an advantage in a small network**

71. OSPF (Open Shortest Path First)
    1. Does not have type of service
    2. Does not have authentication
    3. Does not provide load balancing
    4. **is not better than RIP in small networks**

72. RIP has advantage over OSPF in the following issue
    1. Bandwidth
    2. Type of service
    3. **Memory**
    4. Speed of convergence

73. OSPF has advantage over RIP in the following issue
    1. Computation
    2. **Load splitting**
    3. Memory
    4. Bandwidth

74. SNMP is not used to
    1. Report extraordinary events
    2. Retrieve specific management information
    3. **Transfer mail through the network**
    4. Manipulated management information

75. IP provides
    1. Connection establishment and termination
    2. **Network management**
    3. Flow control
    4. Network access

Data Communications Glossary

A

A/B Signaling - A procedure used in T1 transmission facilities. One bit, fromeach of 24 sub channels in every sixth frame, is used for carrying dial and control information.

Abbreviated Dialing - A feature of some telephone switches which permits users to establish calls by entering fewer digits than the full telephone number.

Access, Access Code - The prefix digits that a telephone user dials to be connected to an outgoing line or trunk.

Access Line - The existing connection between a voice or data customer's equipment and a public communications network. That portion of a leased telephone line that permanently connects the user with the Central Office.

Access Method - Two definitions for "access methods" are currently in use:

1) A CPU resident program built to control the flow of data between central storage and the peripheral devices of a host system. The more common access methods of this type would be IBM 's VTAM, TCAM and BTAM.

2) A method for local area network (LAN) terminals to access the transmission medium. Several types of LAN access methods currently exist: Shared Access, explicit access, contended access and discreet access.

Access Node - Local-Exchange-Carrier owned, Broadband ISDN remote switch which performs grooming, concentration and switching.

ACD (Automatic Call Distributor) - A switching system which automatically distributes incoming calls in the sequences they are received to a centralized group of receivers without human interface. If no receivers are available, the calls will be held until one becomes free.

ACK - This is a control character found in bison protocol. When combined with NAK, the ACK character would indicate that the previously transmit ted data block was correctly received (acknowledge) or incorrectly received (NAK-Negative Acknowledge).

Acoustic Coupler - A kind of modem that uses a standard telephone handset to transmit data over the telephone network. Acoustic couplers are best used in transmitting data at lower speeds (300 Baud) due to the environmental noises present in many office environments, and the acoustic couplers inability to block out the resulting interference.

AC Signaling - A signaling method that relies on alternating current tones or signals to transmit information or control signals.

ACS - An AT&T product (Advanced Communication Service) to provide packet switched Service.

ADCCP (Advanced Data Communications Control Procedures) - USAFS (United States of America Federal Standard) communications protocol, endorsed by the American National Standards Institute.

B

Backup - The hardware and software resources available to recover after a degradation or failure of one or more system components.

Backbone - The major transmission path or facility for a PDN.

Backward Channel - See reverse channel.

Balanced, Balanced Circuit - A network terminated circuit having balanced impedances (between telephone line and network) resulting in a low rate of return loses. Contrast with unbalanced-to-ground.

Band Splitter - A multiplexor (either FDM or TDM) designed to divide a wide bandwidth into several independent, narrower band width channels, for data transmission at a fraction of the total data rate.

Bandwidth - The information-carrying capability of a communications channel or line, expressed in cycles per second (Hz) between the highest and lowest frequencies of a band.

Baseband, Baseband Transmission - Direct transmission method whereby the transmission medium carries only one signal at a time usually for distances under ten miles.

Baseband Modem - A DCE device also known as a line drive or local dataset.

Base Group - Twelve communication VF paths. A unit of frequency division multiplexing FDM) systems bandwidth allocation.

Baud - A unit of signaling speed or rate, taken from the name of French telegrapher, Emile Baudot. Baud is usually defined as the number of signal level changes per second, regardless of information content of those signals. If each signal event represents only one bit condition, baud is the same as bits per second when each signal event represents other than one bit.

Baud Code - A five-bit code set designed for asynchronous transmission of data used primarily for teleprompter systems adding one start bit and 1.5 stop bits . Contrast with ASCII and EBCDIC.

BASIC (Beginners All-purpose Symbolic Instruction Code) - A high- level (many "English-like" terms) programming language.

Batch Processing - A data processing technique where related transactions are grouped together and transmit ted for processing. Contrast with interactive processing.

BCC (Block Check Character) - A control character added to a block in character oriented protocols (such as Bisync) used for determining if the block was received in error -- such as CRC and LRC.

Bit - A contraction of the words: **bi**nary digi**t**, representing the smallest unit of information and the basic unit in data communications. A bit can have a zero or a one value (or a mark or space value in data communications.

Bit Oriented - A communications protocol (such as IBM's SDLC) where control information is encoded in one or more bits. Contrast with byte or character oriented.

Bit Rate - The speed at which binary digits (bits) would be transmit ted over a communications path and usually expressed in "bits per second" (bps). Bit rate should not be confused with Baud which defines the rate of signal state changes.

Bit Stream - The continuous series of transmit ted bits through a transmission link.

Bit Stripping - When referring to statistical multiplexors, bit stripping involves the removal of the start/stop bits on each async character and transmit ting the data using synchronous techniques.

Bit Stuffing - Also known as zero insertion, bit stuffing is a process used in bit - oriented protocols (such as IBM's SDLC) where a string of "1" bits is broken by an inserted "0" bit to avoid confusing data and SYN characters. Once received, the inserted 0 is removed.

C

Cabinet - A physical stand or enclosure designed to rack-mount data equipment and provide easy access to both front and rear panels of the devices contained within. Standard cabinets have 1 3/4" vertical spacing between mounting holes and 19" wide horizontal spacing between mounting rails.

Cable - The combined assembly of one or more conductors within a protective sheath and constructed to permit the use of conductors separately or in groups.

Cable-Based LAN - A local area network (LAN) that uses a coaxial or twisted pair cable as its transmission medium.

Cache Memory - A high-speed computer memory which contains the next most likely instruction or sequence of instructions to be executed upon completion of the present instruction.

Call - A request to connect, or the connection that results from the request, either voice or data. Contrast with minicall and virtual call.

Call Accounting - The recording of data pertaining to start/end times, number of segments, NUI, NTN etc., in packet-switched networks.

Call Detail Recording (CDR) - A PBX feature where each phone call is logged by time and charges.

Called Channel - A channel that can receive but not originate calls. A calling channel can call, but not receive calls, while a called/calling channel can both originate and receive calls. These examples are found in both LAN and packet-switched networks.

Call Forwarding - A telephone service feature that can be programmed to automatically forward calls to another number.

Calling rate - The average number of calls per telephone, determined by dividing the number of busy-hour calls by the number of telephones.

Call setup time - The length of time it takes to establish a switched call between two pieces of DTE.

Card Module, Circuit Card - A printed-circuit board (PC board) designed to plug into a slot in an equipment chassis.

Carrier - A continuous frequency that can be impressed or modulated with a second information carrying signal.

Carrier Detect - An RS-232 interface modem signal (transmitted on pin 8) that indicates that the local modem is receiving a signal from the remote modem. Also called Data Carrier Detect (DCD) and Received Line Signal Detector (RLSD).

Carrier System - The method of transmitting a number of channels over a single path by modulating each channel on a different carrier frequency at the originating end, then demodulating at the receiving end to return the signals to their original form.

Carrier Wave - The wave upon which a signal is superimposed.

Cells - A subdivision of a mobile telephone service area; containing a low powered radio communications system connected to the local telephone service.

Central Office (CO) - The place or building where communications common carriers terminate customer circuits and locate the switching equipment which interconnects those lines. The CO may also be referred to as an exchange, local central office, end office or central exchange .

Central Processing Unit (CPU) - A device designed to execute programmed instructions, perform the logical and arithmetic functions on data and controls input/output functions.

Centralized - Processing with one CPU, which may support remote terminals/job entry stations.

D

DAA (Data Access Agreement) - Any DCE approved by a common carrier that allows privately owned terminals to be connected to the common carrier 's network. Modems manufactured today for the public network have built-in DAA's.

DACS (Digital Access and Cross-connect System) - AT&T central office switching equipment which allows T1 carrier or any of the 64 k bps sub channels to be switched or cross connected to another T1 carrier.

Data - The representation of facts, instructions or concepts in a structured manner suitable for communication.

Data Acquisition - A method of recording and measuring data from physical devices.

Database - An organized collection of information.

Data Channel - The data transmission path between two or more stations.

Data Circuit - A telecommunications medium for the transmission of information in analog or digital form.

Data Collection - A procedure where data arriving from several sources, is combined at one location in a file or queue, prior to processing.

Data Communication - The processes, facilities and equipment used to transport encode d information from one point to another.

Data Dictionary - A listing of all the data names and elements in a system.

Data Encryption Standard (DES) - A cryptographic algorithm endorsed by the National Bureau of Standards (NBS) to encrypt data using a 56 bit key.

Data Entry - The inputting of data into a computer system for processing.

Datagram - A capability in a packet-switched network where a complete message may be contained in the data field of a packet, not usually implemented on today's packet data networks (PDN). See minicall .

Data Integrity - The performance of a data communications system, ideally indicating an absence of undetected errors.

Data Link - The physical connection that includes all necessary equipment for two devices to communicate.

Data Link Control -The management of transmitted data over communications circuits using appropriate hardware and related software.

Data Link Layer - The second layer in the OSI model that establishes, maintains and released data link connections between the network layer and physical layer. While the data link layer is not responsible for error correction, it is responsible for error detection, transmission and reception of datagrams, packet reception and local addressing.

Data Mode - The status of a DSU or modem transmitter where the Request To Send and Data Set Ready circuits are prepared to send data.

Data Network - A telecommunications system consisting of a number of terminals able to access each other via communication lines and switching methods.

Data-Over-Voice (DOV) - A technique used in FDM allowing the combination of voice and data on the same line. DOV usually employs twisted pair cables assigning some of the unused bandwidth for data transmission.

Data PBX - A digital transmission circuit switch allowing users to select from a number of circuit paths. Contrast with PBX.

Data phone - An AT&T trademark identifying the communications equipment furnished by AT&T for data communication service.

Data phone Digital Service (DDS) -An AT&T private line service for transmit ting data over a digital system. The digital technique allows for more efficient use of the transmission facilities, since no modems are required, resulting in lower error rates and costs than with analog systems. AT&T filed for DDS with the FCC in 1974.

Data Service Unit (DSU) - A device used in conjunction with a digital network, replacing the modem in the sense that the DSU provides remote and local testing, loop equalization and the logic and timing needed to provide a standard EIA or CCITT interface. DSU's usually have an integrated Channel Service Unit (CSU).

Data Set - An AT&T trademark synonymous for modem. See modem.

Data speed - An AT&T marketing term used to describe a variety of data communications devices.

Data Stream - The transmission of characters and data bits through a channel.

Data Switch - A device used to connect data processing equipment to network lines, offering flexibility in line /device selection.

Data Terminal Equipment (DTE) - A term used to describe numerous data processing equipment such as computers, terminals, controllers and printers.

Data Transfer Rate, Data Rate - The measure of the speed of data transmission, usually expressed in bits per second. Synonymous with speed, the data rate is often incorrectly expressed in baud .

D bit (Delivery Confirmation Bit) - A bit used in CCITT X.25 packet-switched networks to request end-to-end acknowledgement.

DCD (Data Carrier Detect)

DCE (Data Communications Equipment) -The device installed on premises to provide the functions needed to establish, maintain and terminate a connection as well as the signal conversion required for communications between the DTE and the telephone line or data circuit . Typically, DCE is a modem.

D-Conditioning - A common carrier service designed to control the harmonic distortion and improve the signal-to-noise ratio. D-conditioning is currently being offered in 9600 bps service with complex modems on voice grade private lines.

DDCMP (Digital Data Communications Message Protocol) - A DEC data communications line protocol.

DDD (Direct Distance Dial) - The North American telephone dial system enabling users to call subscribers outside of their local area without operator assistance. In the United Kingdom and other countries, the service is known as STD (Subscriber Trunk Dialing).

DDS (Data phone Digital Service) - A digital service offered on private lines and eliminating modems. DDS is offered inter-LATA by AT&T (as an ACCUNET offering) and intra-LATA by BOC's.

E

Earth Station - The transmitter and related antenna located on earth for communication with a satellite.

EBCDIC (Extended Binary Coded Decimal Interchange Code) - An 8- bit character code, standard for many IBM systems offering 256 possible combinations of characters.

Echo - The reflection or return of transmitted data.

Echo Cancellers - A device to suppress echo's (similar to an echo suppressor) without speech clipping and able to operate during two-way transmissions.

Echo Check - A method of checking for data transmission errors by returning the received data to the sending end for comparison with the original data.

Echo Distortion - Impairment in telephone lines caused by electrical reflections located at distant points where line impedances are dissimilar.

Echoplex - One method of checking data integrity by returning characters to the sending station for verification. This process requires simulated full duplex operation.

Echo Suppressor - A device used by telephone companies to block the receive side of the line during the time that the transmit side is in use.

ECMA (European Computer Manufacturers Association) - A trade organization and member of the ISO issuing data communications standards. Its membership includes western European computer manufacturers and suppliers.

EEPROM (Electrically Erasable Programmable Read-Only Memory) - A PROM that can be cleared or erased using electrical signals rather than the ultraviolet light required for EPROM.

EFS (Echo Free Seconds) - The measurement, in seconds, of the percentage of time data is transmit ted error free.

EIA (Electronic Industries Association) - A trade association recommending data communication standards, with RS-232 the best known. EIA is comprised of American electronics manufacturing corporations and also contributes to ANSI. See ANSI.

EIA Interface - Data transmission signal characteristics designed with universal standardization for data communication including duration, current and voltage for hardware devices. See also EIA.

Electronic Mail - The delivery of mail or messages, either all or in part via a public or private data communications system.

Electronic Switching System (ESS) - A computerized, digital telephone switching system, manufactured by AT&T, utilizing a stored program to control the switching function. With ESS, custom calling features such as Call Waiting, Call Forwarding and Three-Way calling are available to the subscriber.

EM (End of Medium) - Also known as End of File, the EM character is sometimes used to indicate the physical end of data recorded on a medium .

EMI (Electromagnetic Interference) - A level of undesirable radiation or interference, oftentimes reduced through the use of shielded cables. The FCC has defined acceptance levels for EMI.

Empty Slot Ring - A LAN environment practice whereby an empty packet would circulate through each station in a LAN ring. A single bit within the header of the packet indicates if messages are present and, if so destination and source addresses are also contained within.

Emulation - Designing a device or program to perform or imitate something else, i.e.; IBM 37XX emulation or IBM 3270 emulation.

Encoding, Decoding - Formatting data into a pattern suitable for data communication.

Encryption - A method of data protection whereby a bit stream would be changed to include additional bits, or appear as a random sequence of bits to an unauthorized observer.

End Office - The first central office that a subscriber's telephone line is connected to over the access line. Also, the end switching office for a dialed connection.

ENQ (Enquiry) - A control character used in the ASCII code set to request identification status.

EPROM (Erasable Programmable Read Only Memory) - A form of computer memory that is non-volatile but may also be erased via the use of ultraviolet light for reuse. See EEPROM and PROM.

Equalizer - A capacitor or coil like device used by modems to compensate for distortions caused by telephone line conditions.

Equalizer, Adaptive - An equalizer able to change dynamically to compensate for distortion caused by telephone line conditions.

Error - A term used to describe a deviation from the expected, especially if data integrity is jeopardized.

Error Correction - A method to insure data integrity in received data, performed by retransmission requests to the sending station (source), or by manipulating the received data. See ARQ and FEC.

Error Rate - The measure of data integrity given as the blocks, bits or characters incorrectly received, versus the number transmit ted. Error rate is sometimes seen as a rate of one error every one million bits.

ESS - See electronic switching system.

Essential Facilities - A term used in packet switched environments to define the standard facilities found on all networks . Compare with additional facilities.

Ethernet - The de facto standard LAN of the Xerox corporation and later sponsored also by DEC and Intel Corp. Characterized by 10 m bps baseband transmission using CSMA/CD, Ethernet uses coaxial cable and is similar to the standard LAN recommended by IEEE 802.3.

ETX (End of Text) - A control character preceding a BCC, indicating a message conclusion.

Exchange - One or more central offices and equipment belonging to the telephone company designed to administer communication service to a particular area.

Exchange, Private Automatic (PAX) - A privately operated dial telephone exchange designed to prohibit calls to or from the public telephone network.

Exchange, Private Automatic Branch (PABX) - A user owned (private) automatic telephone exchange that may be a data PABX, voice PABX or voice/data PABX.

Expander - A transducer-like device with the capability to expand the input voltages for a given range of amplitude.

Explicit Access - Contrasted with contended access, explicit access is a method of shared access found in LAN environments, allowing stations to make use of the network individually for a certain time period. Each station receives a turn, but must also wait for its turn.

F

Facility - Two definitions exist in networking technology:

1) The computer system capabilities due either to software or hardware.

2) The data communications lines and equipment required to build a circuits and transmission networks.

Fading - Interference from radio transmission signals or microwave communication causing a received signal to deflect from the target.

Far-End Crosstalk - Crosstalk interference occurring in the same direction as the signal. Contrast with near-end crosstalk.

Fast Select - A packet-switched transmission method whereby the user is able to transmit small amounts of data (approx. 128 characters) with the call request packet, instead of transmit ting the data information in packets following the call request packet. This method allows a user to have small amounts of information arrive at the destination quickly.

FAX (Facsimile Terminal) - An image transmission system designed to reproduce the communicated image (such as documents or photographs) on a paper forms.

FCC (Federal Communications Commission) - A board of seven presidential appointees empowered to regulate all USA interstate communications systems as well as all overseas communications originating or terminating in the USA. The FCC was created by the Communications Act of 1934.

FCS (Frame Check Sequence) - A method for error detection in bit-oriented protocols, normally consisting of a 16-bit fields.

FDM (Frequency Division Multiplexing) - A method of multiplexing where a data lines bandwidth is divided into channels and assigning a specific range of frequencies to each channel.

FDX (Full Duplex) - Transmitting data in both directions simultaneously. FDX can occur on either two or four wire circuits.

FE (Format Effecters) - The control characters used to control information displayed on a monitor or printer.

FEC (Forward Error Correction) - The inclusion of additional data contained in a transmit ted block, to be used by the receiver in case of errors.

FEP (Front-End Processor) - A data communications device designed to offload the host processor from the task of message routing between application programs and user terminals, error correction and other communications processing functions.

FEX, FX (Foreign Exchange Service) - A service designed to connect the subscriber's telephone to a remote exchange, providing what appears to be local telephone service. May be a virtual service.

FF (Form Feed) - A control character found in both ASCII and EBCDIC code sets requesting a printer to advance to the top of the next page or form.

Fiber Loss - The weakening of light signal strength in fiber optic transmission.

Fiber Optics, Fiber Optic Cable - A transmission medium using plastic or glass fibers to carry light rays containing information. See optical fibers.

Field - A reserved area of a display monitor for a specific type of information. Also, a component of a data base record.

Figures Shift (FIGS) - A control character used in the Baud Code to enable the printing of symbols and numbers by actually allowing a physical shift of the carriage. See also Letters Shift.

File - A collection of related data records directed toward some purpose and sequenced in a particular manner.

File Server, File Server protocol - A LAN station or protocol designed to allow application programs to share and store data files.

Filter - The electronic device or devices used to attenuate undesirable signals within frequencies in the transmission circuits and pass through, unchanged, desirable signals within frequencies.

FIPS (Federal Information Processing Standard) - A US government approved standard for computer processing and data communications.

Firmware - The software designed within hardware devices, usually permanently stored in a ROM or PROM chip. Firmware may also be temporarily stored within an EEPROM or EPROM chip, as well.

Flag - A field used in bit-oriented protocols where a character or bit field would be used to separate the data on either side of the flag.

Flat Rate Service - A telephone service available in certain geographic areas, entitling the subscriber to an unlimited number of calls within a predefined area for a fixed rate.

Flow Control - A method of preventing the loss of data whereby the transfer of messages or characters to a receiving device would be controlled via the use of a control character (s) such as X-ON (transmit on) or X-OFF (transmit off), allowing the receiving devices buffer to drain before accepting more data.

FM (Frequency Modulation) - One of three different methods of transmit ting digital information on an analog line. FM changes the carrier frequency to different values. Also see AM and PM.

Foreign Attachment - Any equipment not owned or provided by the telephone company, but attached to the telephone companies lines. See also CPE.

Flag - A field used in bit-oriented protocols where a character or bit field would be used to separate the data on either side of the flag.

Flat Rate Service - A telephone service available in certain geographic areas, entitling the subscriber to an unlimited number of calls within a predefined area for a fixed rate.

Flow Control - A method of preventing the loss of data whereby the transfer of messages or characters to a receiving device would be controlled via the use of a control character (s) such as X-ON (transmit on) or X-OFF (transmit off), allowing the receiving devices buffer to drain before accepting more data.

FM (Frequency Modulation) - One of three different methods of transmits ting digital information on an analog line. FM changes the carrier frequency to different values. Also see AM and PM.

Foreign Attachment - Any equipment not owned or provided by the telephone company, but attached to the telephone companies lines. See also CPE.

G

Gain - A decibel (dB) measurement of amplitude. The gain is amplified whenever the signal passes through a repeater, antenna or amplifier.

Gain Hits - Any form of undesirable signal surge resulting in the possibility of corrupted data. AT&T standards suggest a maximum permissible threshold of less than eight gain hits within a fifteen minute period.

Garbage - A slang term often used to describe corrupted data.

Gateway - A network station designed to interconnect two otherwise incompatible devices or networks. Occasionally, a gateway may perform protocol conversion and packet assembly/disassembly (PAD) functions. Gateways operate at the fourth through seventh layers of the OSI model. Contrast with bridge .

Gaussian Noise - A line noise whose amplitude is characterized by the Gaussian distribution such as white noise, ambient noise or hiss.

General Switched Telephone Network (GSTN) - Same as public telephone network (PTN).

Geosynchronous, Geostationary - The path of an orbiting communications satellite at the correct speed and distance over the earth so as to appear stationary as the earth rotates.

GFI (Group Format Identifier) - The first 4 bits in a packet header (X.25 packet-switched networks) containing the D bit, Q bit and modulus value.

GHz (Gigahertz) - A measurement of frequency equal to 10 to 9th power.

Grade of Service - A percentage measurement of incomplete, delayed or blocked calls.

Ground - The electrical common conductor.

Ground Start - A method of signaling designed to detect that a circuit is grounded at the far end.

Ground Station - Also known as an earth station, a ground station is designed to send (transmit) and receive signals to and from a communications satellite.

Group Addressing - Any address that is shared by two or more devices or stations.

Group Channel - An organization on telephone carrier systems, whereby a full group is a channel equivalent to 12 voice grade channels at 4000 Hz for a total of 48 kHz . A half-group has the equivalent bandwidth of six voice grade channels (24 kHz). By not subdividing into voice grade facilities, group channels can be used for high-speed data communication . See also wideband.

Guard Band, Guard Frequency - Two definitions are commonly found in data communications:

1 - The unused frequencies between sub channels in FDM systems used to separate channels, thereby preventing crosstalk.

2 - A single carrier tone used to indicate that a communications line is prepared to transmit data.

H

Half-Duplex Transmission (HDX) - The common use definition is a circuit designed for transmission in either direction but not both directions simultaneously. Contrast with FDX, full-duplex transmission.

Hamming Code - A method of forward error correction (FEC) named for its inventor and designed to detect and correct a single bit received in error.

Handset - The part of a telephone that contains both receiver and mouthpiece.

Handshaking, Handshake - Communications line interplay used to establish a data path via the exchange of predetermined signals, usually performed by communications protocol or modems.

Hardcopy - The printed output of a computer, in readable form.

Harmonic - The frequencies that combine as multiples of some basic or fundamental frequency.

Harmonic Distortion - An impairment of a transmission line caused by erroneous frequency generations along the line.

Hardware - The physical equipment that comprise a computer system, including mechanical, or electromechanical devices, as opposed to the computer program. Contrast with software .

Hardware Interface - Physical hardware used in the inter connection of computer/data terminal devices and modems.

Hardwired - The permanent connection of data communications links, lines or cables and related devices.

Hardwired FEP - A non-programmable front-end processor (FEP).

HASP (Houston Automatic Spooling Priority) - Also known as Job Entry Subsystem (JES), HASP is a control program adopted by IBM for the transmission of jobs to computers and the control of devices and data lines.

HDLC (High-level Data Link Control) - A bit protocol developed by the ISO to be the international standard communications protocol, similar to IBM 's SDLC.

Head-End Unit - A LAN environment hardware device found on a broadband network that uses separate frequencies for multiple services.

Header - The control block or blocks of data added prior to the actual message, either a packet or a transmission block.

Hertz (Hz) - The same as cycles per second, used as a measurement of bandwidth or frequency.

Hexadecimal - A base 16 numbering system representing the states as 0 through 9 followed by A through F. Any eight-bit byte can be represented by two hexadecimal digits.

Hierarchical Network Structure - A network plan whereby all functions are categorized into specific areas or layers, each having a specific role.

Hierarchical Switching - Used to describe a switching methodology used in LAN’s where the switching is done in stages. In a star topology, this is called star switching.

High Frequency (HF) - Any frequency level that falls in between 3 and 30 mHz.

High Pass - A predetermined filter frequency level, above which all frequencies may pass. Contrast with low pass.

High Performance Option (HPO) - An alternate means of conditioning a communication circuit, similar to D1 conditioning.

Hit, Line Hits - A slang term or expression to describe line noise or other forms of interference causing data communications line failure or corrupted data.

Holding Time - The time it takes to establish a telephone connection. Factors include telephone equipment, busy periods, etc.

Horizontal Redundancy Checking (HRC) - A method for data error checking whereby redundant information would be included in the data to be checked. Contrast with LRC (Longitudinal Redundancy Checking).

Host, Host Computer - The central or controlling computer in a data communications network, usually providing database access, programming languages, etc.

Hub - A DDS office designed to multiplex T1 data streams from a number of local offices into signals suitable for transmission.

Hybrid - Any combination of two or more technologies. For example, DDCMP is a hybrid character/bit data communications protocol.

I

IBM (International Business Machines Corp.) - One of the leading computer hardware and software manufacturing companies in the world, having many de facto standards such as the IBM PC and 3270 terminals.

IC (Integrated Circuit) - Also known as a microchip, and as a semiconductor device, an IC performs numerous functions in data processing such as processing, data storage and program storage. See also PROM, EEPROM, EPROM, ROM and RAM.

IDF (Intermediate Distribution Frame) - A connecting frame or such device used to connect data communications equipment by the use of connecting blocks.

Idle Character - Similar to SYN character and NUL character.

IEC (Interexchange Carrier) - An FCC licensed common carrier permitted to carry subscribers transmissions inter- LATA, or if approved by a PUC or PSC, intrastate.

IEEE (Institute of Electrical and Electronic Engineers) - An international institute that issues its own standards and is a member of ANSI and ISO, perhaps best known for its development of IEEE Project 802. Click here to visit the IEEE web site.

IEEE Project 802 - The IEEE development team credited with the creation of the 802 series of local area network (LAN) standards.

IEEE 802.2 - A LAN standard for the data link layer used with other Project 802 standards such as IEEE 802.3, IEEE 802.4, IEEE 802.5. See also: ISO.

IEEE 802.3 - A LAN standard for the physical layer using the CSMA/CD access method, similar to Ethernet, within a bus topology. See also: ISO.

IEEE 802.4 - A LAN standard for the physical layer, using a token- passing access method within a bus topology and functioning similarly to MAP. See also: ISO.

IEEE 802.5 - A LAN standard for the physical layer, using the token ring or token passing access method on a ring topology.

IEEE 488 - An IEEE standard parallel interface, oftentimes used to connect data communications equipment using connecting blocks.

Impedance - The signal effects due to a varying current, resistance capacitance and inductance. Line impedance (ac resistance), if increased via inductance will allow a greater amount of power to be transmit ted with less current, but at a higher voltage.

Impulse Noise - A communications line interference caused by electrical action, lightning, on/off movement of switching equipment, etc., and appearing as high amplitude and short duration.

Impulse Hits - Also known commonly as "spikes", impulse hits are errors of impulse noise adversely affecting data communication. AT&T recommends no greater than 15 impulse hits per 15 minute period.

IMS/VS (Information Management System/Virtual Storage) - An IBM software product designed for both batch processing and data communications-based transaction processing.

Induction, Inductance - A method of loading a circuit or line to help reduce attenuation at voice frequencies (VF).

Information - Raw data that has been organized into a meaningful context for a computer user.

Infrared - A method of data transmission using infrared light to transmit data on fiber optic medium or open-air transmission over short distances.

Information Bit - A data bit, having value as a component of a message or text, as opposed to an overhead bit used for addressing or error control.

Input/output (I/O) - Moving data between a peripheral device and the CPU, or simply a term used to describe a type of peripheral device.

Insertion Loss -The loss of signal power due to the connection of communications units possessing different impedance values.

Integrated Circuits - A complex electronic circuit providing all the capability of circuits containing resistors, diodes, capacitors, etc., and remaining functionally equivalent without these components.

Integrated Services Digital Network (ISDN) - A CCITT standard for digital communication systems designed to transmit voice, data, video and other digital communication having major effects on the design of multiplexers and other communication equipment.

Intel - A microchip manufacturer and one of the sponsors along with Xerox Corp., of Ethernet.

Intelligent, Intelligence - A term used to describe a microprocessor controlled device able to perform sophisticated tasks relying on software, and therefore programmable.

J

Jabber, Jabbering - The flow of continuously sent garbage from a failed terminal, resulting in a lockup of a LAN for other users.

Jack - Either a three-conductor or a "mini-plug", RJ11 type receptacle designed to accept the corresponding plug for an electrical connection.

Jamming - The disturbance or interference of open-air radio transmission to deliberately prevent communication.

JES (Job Entry Subsystem) - The control program and procedure for directing host processing of a job or series of jobs and related tasks in an IBM host environment.

Jitter - One form of line distortion caused when a transmit ted signal deviates from its reference timing position, causing errors, especially in high speed transmission.

Job - A set of data, including programs, files and instructions to a computer known as Job Control Language (JCL, in the IBM realm).

Jumbo Group - The highest frequency division multiplexing (FDM) carrier system multiplexing level that contains 3600 voice frequency (VF) or telephone channels in six master groups and also known as hyper group.

Jumper, Jumper wire - The wire/wires used to cross-connect circuits for testing or diagnostic purposes.

K

Ka Band - The frequencies used for satellite communications, approximately in the 30/15 gHz range.

Kbps (Kilo Bits Per Second) - Thousands of bits per second (BPS) equal to 10 to the third power. See also BPS.

Keying - A method of encoding data by modulating the carrier either by phase or frequency.

KHz (kilo Hertz) - Abbreviation for 1000 Hertz (cycles per second). See also Hertz.

KSR (Keyboard Send and Receive) - A teleprompter transmitter and receiver that can only transmit from the keyboard. Contrast with RO and ASR devices.

Ku Band - The frequencies used for satellite communications, approximately in the 14/12 gHz range.

L

LADT (Local Area Data Transport) - A common-carrier offered communication service that transmits both voice and 4800 bps data simultaneously over the same telephone line.

LAN (Local Area Network) - The data communications facilities used to provide communications within a limited geographical area, normally up to 6 miles, using medium to high data rates between 9600 bps to 100 mbps. LAN 's may have bridges or gateways to other networks but are usually confined to a building or cluster or buildings, frequently referred to as a "campus".

LAP (Line Access Procedure) - A term used in packet-switched networks to define the data-link layer level protocol specified in the CCITT X.25 interface standard, superseded by LAPB.

LAPB (Line Access Procedure, Balanced) - A term used in packet- switched networks to define a link initialization procedure designed to establish and maintain communications between the DTE and DCE. All PDN's currently support LAPB, which involves the T1 timer and N2 count parameters.

LASER (Light Amplification by Simulated Emission of Radiation) - A fiber optic method of data transmission using very high frequency beams of light with great information carrying capacity.

LATA (Local Access and Transport Area) - A divestiture related subdivision that resulted in approximately 184 local telephone serving areas in the United States. The areas of LATA 's are designated primarily by demographics, and are distinguished separately from long-distance service.

Latency - The waiting time, or delay between a stations request to a transmission channel, and completion.

Layer - A term used to define one level of a hierarchy of functions, as specified by the OSI reference model. Divisions of other protocols, such as IBM 's SNA, sometimes will correspond to one or more OSI layers.

L Band - The microwave transmission frequencies approximately in the 1 GHz range.

Leased Line, Private Line, Dedicated Line - A point-to-point or multipoint communications line for voice/data leased from a common-carrier, usually on a monthly basis.

LED (Light Emitting Diode) - An electrical component, offering greater reliability than an ordinary bulb, used to indicate status information. LED's are also used as a fiber optic transmission source.

Letters Shift - A control character used in the Baud Code to enable the printing of alphabetic characters. See also figures shift.

Light Wave - Fiber optic transmission using very high frequency light beams.

Line - A multipoint or point-to-point communications medium.

Line Discipline - An archaic term for line protocol.

M

MAC (Media Access Control) - An access control protocol defined under IEEE 802 which includes variations for the token ring, token bus and CSMA/CD.

Magnetic Medium - Any medium designed for data storage using magnetic pulses to record information, such as magnetic tape, diskettes or disks.

Mainframe - A large-scale computer, capable of processing large amounts of data with very fast processing, including control units and peripheral devices supplied by one vendor, examples of which would include IBM, Unisys, Control Data, and others. Often, mainframe systems will have a closed architecture.

Main Network Address - A term used in IBM's SNA to define the logical unit (LU), network address, within VTAM.

Manchester Code, Manchester Encoding - A binary signaling mechanism in which each bit period is divided into two complementary halves, combining data and clock pulses.

MAP (Manufacturing Automation Protocol) - A General Motors Corp. token-passing bus designed for factory environments that appears very similar to IEEE 802.4.

Marginal Relay - A relay designed to operate only on a specified current flow which is greater than the current normally flowing in the circuit.

Mark - Three definitions exist in normal usage:

1) In telegraph communications, a mark indicates the closed, current -flow condition.

2) When used in data communication, a mark indicates a no-traffic state for asynchronous transmission, a binary 1.

3) A mark may also indicate the idle condition, contrast with space. See mark-hold.

Mark-Hold - Transmitting a steady mark to indicate the normal no- traffic line condition.

Mark-to-Space Transmission - Switching from a marking impulse to a spacing impulse.

MASER (Microwave Amplification by Simulated Emission of Radiation) - A device designed to generate a microwave signal with low-noise properties.

Master Clock - The timing signal or signal mechanism used by all stations in a network for synchronization.

Master Group (MG) - A term used in Frequency Division Multiplexing (FDM) whereby an assembly of 10 super groups (600 voice frequency channel s) would occupy adjacent bands in the transmission spectrum to provide simultaneous modulation and demodulation.

M Bit - An X.25 bit that notifies the receiver that all data from the sender has been transmitted.

Mbps - Millions of bits per second (bps).

Mean Time To Failure (MTTF) - The average duration of periods for which the system, or a related component, functions without fault.

Mean Time Between Failures (MTBF) - See mean time to failure.

Mean Time To Repair - The average length of time required to fix the equipment or system. See mean time to failure and availability.

Medium - The material used to record or transmit data.

Message Routing - Selecting a path or channel for message transmission.

Message Switch, Switching - A device and the related process for receiving, storing and, upon the availability of a line or receiver, retransmitting the message. See also store-and-forward.

Message Telephone Service (MTS) - The official designation for tariffed toll telephone service.

MHz (Megahertz) - A unit equal to one million cycles per second (Hz).

Microcomputer - A small desktop or lap-top computer often called a personal computer.

Microprocessor - The processing unit of a microcomputer sometimes called a "computer-on-a-chip".

Microprogramming - The practice of building a program into ROM to carry out functions otherwise contained on a storage device and processed at a substantially slower speed.

Microsecond - One millionth of a second.

N

NAK (Negative Acknowledgment) - Two primary uses are encountered for this control character :

1) In the BSC protocol, NAK indicates and error in the previous transmission block and that the receiver is ready to accept retransmission. Contrast with ACK.

2) NAK represents the "not ready" reply to a poll on a multipoint system.

Nanosecond - One billionth of a second.

National Facilities - A packet-switched environment nonstandard facility selected for a given nations network, and may or may not be found on other networks.

NBS/ICST (National Bureau of Standards/Institute for Computer Sciences and Technology) - The Gaithersburg, Maryland bureau assigned to develop data communications and computer processing FIPS (Federal Information Processing Standards). Membership includes other USA government agencies and network users.

NCC (Network Control Center) - An office or station assigned the task of data network diagnosis.

Near-End Crosstalk (NEXT) - Crosstalk occurring at the source of the transmit ted signal.

Network - Generally, a network can be said to be any inter-connection of computer systems facilities (including control units, modems, terminals, etc.) although three network categories exist in common usage:

1) Switched networks, in which the telephone network is the telephone lines normally used for dialed telephone calls for voice or data.

2) Any series of points connected by communications channels.

3) Dedicated, Leased or Private networks, reserved for the use of one user or customer.

Network Addressable Unit (NAU) - A host based physical unit (PU), logical unit (LU), or system services control point (SSCP) in the IBM SNA environment.

Network Architecture - The hardware and software plan of configuration for a computer network by a particular manufacturer or vendor.

Network Communications Control Facility (NCCF) - A host based IBM program allowing users the ability to monitor and control network operation.

Network Control Program (NCP) - A FEP -resident program designed to handle communications control and function as an interface between the data communications network and host processor.

Network Facilities - A term used in the packet-switched environment used to describe two forms of standard facilities:

1) The "essential" facilities found on all networks.

2) "Additional" facilities which may be present on one network, but omitted on another.

Network Interface Machine (NIM) - A form of protocol converter used to adapt an X.25 packet network with non- packet mode terminals.

Network Layer - The third entity in the OSI model that is responsible for addressing and routing between sub networks and servicing the transport layer.

Network Problem Determination Application (NPDA) - An IBM host- based program designed to aid in the isolation and diagnosis of network problems.

Network Services - The service within the NAU's of an IBM SNA environment controlling network operations through sessions to and from the host SSCP.

Network Terminal Option (NTO) - An IBM SNA environment program that allows non-SNA asynchronous and BSC devices access to the network via the communications control unit (3705/3725/3745).

Network Topology - Outlining all network nodes and their physical/logical relationship, such as ring, bus, star, etc. See topology definition.

Network Virtual Terminal - The usage of numerous data terminals having different protocols, formats, data rates and codes on the same network.

Neutral Current Loop - See current loop.

Nibble - The last or first four bits of an eight bit byte.

Node - An inter-connection point to a data communications network, however, examining further, the following definitions also apply:

1) In a packet-switched environment, one of the switches that forms the networks backbone.

2) Any unit that is polled on a multipoint network.

3) A LAN station or any unit on a ring topology.

Noise - The random electrical signals, a communications line impairment which can either be inherent in the line design or induced by natural disturbances and therefore corrupting transmitted data.

Noise Suppressor - A device designed to minimize or eliminate noise in a data communications circuit by means of signal processing or filtering. See filter.

Non-Blocking - The permanent connection of a device through a switching mechanism where, regardless of the switch setting, a continuous path exists to that device.

Non-Erasable - Computer memory or storage that is not erasable. See ROM.

Non-Impact Printer - A printing device using either heat (thermal), light (laser), or other means (such as electrostatic), to produce printed output rather than a mechanical striking action.

Non-Interactive System - A computing system where the computer functions independently of the user during program execution.

Non-Linear Distortion - A form of line

distortion sometimes referred to as "clipping" caused by signal level attenuation.

Non-Persistent - A term used in a LAN environment to define a CSMA method where, in the event of a collision, the stations do not attempt an immediate retransmit, even if the communications network is quiet. Compare with persistent.

Non-Transparent Mode - A mode of bison protocol where control characters and sequences are recognized through the examination of all transmit ted data. Contrast with transparent mode.

Non-Volatile - Computer memory or storage that would not be lost once the power is turned off to the memory or storage device. See ROM .

Normally Closed/Released Contacts -The closed or open contacts on a unoperated relay.

O

Object Code - An executable machine code, the result of the output of a translating program such as an assembler or a compiler. Contrast with source code.

Octal - An eight state (0-7) digital system.

Octet - A grouping of 8 bits, similar but not identical to a byte, found in packet-switched environments.

Off-Hook - An activated telephone set or a modem automatically answering a call. Contrast with on-hook.

Office Automation - A term used to describe the wide use of mechanized systems in the office environment, typically including LAN 's, word-processing/desk-top publishing, electronic mail, shared databases, etc.

Off-Line, Offline - Any equipment or devices not accessible to the CPU . Also, any terminal equipment not connected to a transmission line. Contrast with online.

Off Loading, Off Loaded - A process whereby a device is relieved of certain processing tasks, so that another (possibly less expensive) device can fill in those duties. Example: a FEP offloads a host processor or a terminal may off load a concentrator.

Off-Net - A term used to define any location that is beyond the primary serving area of a DDS. Contrast with on-net.

1-Persistent - A term used in a LAN environment. See persistent.

On-Hook - A deactivated telephone set or a modem that is not in use. Contrast with off-hook.

On-line, Online - Any computer equipment or devices that are accessible to the CPU. In the case of an online system, input data can enter the computer directly from their point of origin, or output data can be transmitted directly to where they are to be used.

On-Net - A term used to define any location that is beyond the primary serving area of a DDS. Contrast with off-net.

Open-Air Transmission - A data communications technique relying on radio frequency (RF) signaling, including infrared, microwave and FM radio.

Open Wire - The description used to define a transmission conductor(s) supported separately above the grounds surface, such as a telephone cable supported on insulators by a telephone pole.

Operand, Operands - The entity on which operations are performed.

Operating System (OS) - The fundamental control program of a computer consisting of tasks or processes used in various supervisory and control functions to perform:

1) Hardware device allocation

2) Access to software resources-e.g., file editors, compilers, assemblers, subroutine libraries and utility programs.

3) Protection functions, that is, access control and security for information.

4) A means of communicating messages or signals among tasks.

Operation Code, Op Code - The part of a computer instruction which specifies what operation has to be performed on the operands.

Optical Fiber - The thin filaments of glass, glass strands or glass-like material, each of which is an independent circuit for transmission of very wide frequency ranges. Optical fiber is contained in a shielded fiber optic cable for communications use.

OSI Model (Open Systems Interconnection Model) - The 7-layer reference model recommended by the ISO to provide a logical structure for network operations protocol.

Other Common Carrier - A term used to include domestic and international record carriers (IRC's), specialized common carriers (SCC's), and domestic satellite carriers, authorized to provide leased line services competitively with established telephone common carriers.

Overhead - The transmitted information used in addressing control, routing and error detection that is sent in addition to a users transmit ted data.

Overhead Bit - A bit used for data communications overhead . Contrast with information bit.

Overrun - The data loss resulting from a receiving device that is unable to accept data at the speed of the transmit ting device.

Oversampling - A method used in TDM whereby each bit from each channel is sampled more than once.

Over speed - A situation whereby transmitting devices, such as modems and PABX's would operate at a slightly faster speed than the data sent for transmission. Typically, modems and PABX's have over speeds of 0.1% and 0.5% respectively.

P

PABX (Private Automatic Branch Exchange) - See exchange, private automatic branch.

Pacing Group - A term used in an IBM SNA environment to define the number of data units that can be sent before a response.

Packet - A group of information and overhead bits sometimes referred to as a message, that is transmitted as a package on a packet-switched network, and is usually smaller than a transmission block.

Packet Assembly Unit - A device or facility attached to a packet system to allow non packet-mode terminals to transmit and receive data with packet-mode terminals.

Packet Header - A term used in a packet-switched environment to describe the first three octets of an X.25 packet.

Packet Switching, Packet-Switched Network - The sending of addressed packets containing data over a data communications network via a channel occupied for the duration of the packet transmission. Packets from different sources would be interleaved over channels (called virtual circuits).

Packet Terminal - Any DTE device able to transmit and receive packets.

PAD (Packet Assembler/Disassemble) - A device used in an X.25 packet-switched environment to interface non-X.25 devices to an X.25 network . A PAD would assemble/disassemble packets and may be synchronous or asynchronous with single or multiple channels.

PAD Character - A character normally sent at the beginning/end of a synchronous transmission to provide timing and bit synchronization.

Paper Tape - An archaic input/output medium on which data would be recorded as a pattern of five or eight channel punched holes.

Parallel Interface, Parallel Transmission - The interface or process designed to send each bit simultaneously over a separate line or wire, and usually used to send data one byte at a time to a high-speed printer or local peripheral. Contrast with serial interface, serial transmission.

Parallel Processing - True parallel processing involves the processing of more than one task on a computer system, within the same processor.

Parity, Parity Check - Parity is a term synonymous with equality. Parity checking is an extensively used error-checking facility provided to insure correct recording of data, its input into a computer system, and its transfer within the system, including networks and data communication. A parity check consists of adding up the bits in a unit of data, calculating the parity bit required, and checking the calculated parity bit with that transferred with the data item. This form of check will normally be performed by a hardware device.

Parity Bit - An error-checking bit whose binary value (0 or 1) depends on whether the sum of bits with the value 1 in the unit of data being checked is odd or even. If the total number of bits with value 1, including the parity bit (or bits), is even, the unit of data is said to have even parity; if it is odd, it has odd parity. Error checking methods use either even or odd parity. The data communication system or network will use the same parity principle, even or odd throughout. Any error caused by incorrect parity detected as a result of a parity check is called a "parity error". The unit of data to which a parity check is applied may be a character, a byte, a word, etc., the character parity check being the one most often used. The smaller the unit of data to which the check is applied, the higher the probability that compensating errors will not occur.

Parity Check, Horizontal - A method for performing a parity check, also known as LRC (longitudinal redundancy check) where a parity check is applied to a group of particular bits from each character in a block.

Parity Check, Vertical - A method for performing a parity check also known as VRC (vertical redundancy check) where a parity check is applied to a group which is all bits in one character.

Parity Error - A data error where an extra or missing bit is detected.

Part 68 - That portion of the FCC regulations permitting the registration of voice/data communications equipment provided they meet federal requirements designed to ensure no harm to the telephone network.

Partitioned Emulation Programming Extension (PEP) - IBM software used with the Network Control Program (NCP) to permit a communications controller to operate in partitioned mode, controlling an SNA network while managing a number of non-SNA communications lines.

Pass Band Filters - A filter used to allow only certain frequencies within the communications channel to pass while rejecting all frequencies outside the pass band. Such filters may be internal to the modem or a separate device.

Patching Jacks - A series-access hardware device or cable, used to patch or bypass faulty equipment by using any available spare units.

Path Control Layer - The network processing layer, in an IBM SNA environment, handling the routing of data units through the communications network and also managing shared link resources.

Q

QTAM (Queued Telecommunications Access Method) - An IBM data communications access method designed to provide the capability of BTAM plus the added feature of message queuing on direct access storage devices (DASD). QTAM is used for data collection, message switching and many other data communications uses.

Quad - A cable containing two twisted pairs of conductors.

QAM (Quadrature Amplitude Modulation) - The process of combining both amplitude modulation and phase modulation techniques to provide more bits per baud.

Quadrature Distortion - The distortion of an analog signal often occurs in phase modulation.

Queue - A "waiting line" of items or units, such as messages, waiting to be serviced.

Queuing, Queuing Theory - A process allowing transactions to be serviced and specifies each of the following elements:

1) Source- The electronic signals of a data communications system.

2) Input Process- The statistical pattern by which the data arrives at the service facility, also called "random arrivals".

3) Queue Structure- The actual "waiting line", which may consist of one queue or several queues. The line(s)" may be conceptual rather than physical, such as the case of remote terminals waiting to be polled by a computer.

4) Service Facility- One or more service channels in parallel, attached to one or more servers in series.

5) Service Process- The time required to completely service a unit waiting in a queue. The time is determined by probability formulas.

6) Service Discipline- The rules by which units are selected and serviced. Service may be FIFO (first in, first out), random, or according to some priority procedure.

R

Rack Mount - A term used to describe devices designed to fit a data cabinet, sometimes in a "modular" fashion.

RAM (Random Access Memory) - A storage device into which data may be entered and read, usually (but not always) a volatile semiconductor memory.

Rate Center - A defined geographic point used by telephone companies for distance measurements for inter- LATA mileage rates.

RBT (Remote Batch Terminal) - An input/output terminal designed to operate in a RJE location for transmit ting and receiving data from a remote processor in batch processing form.

RD (Received Data) - An RS-232 data signal, received by a DTE device from a DCE device on pin 3.

Reactance - A frequency sensitive data communications line impairment causing phase shifting and a loss in power.

Real Time, Real-Time System - A real-time system responds immediately at the time a transaction occurs, unlike a batch processing system which would produce journals, reports, and other outputs according to prescheduled batch processing cycles. Real-time systems in which there is rapid and frequent interaction between human and machine are sometimes said to operate in a "conversational" mode.

Reasonableness Checks - A testing method designed to ensure that data reaching a real-time computer or being transmitted from it is within a specified range. This process, also known as a "limit check" is a means of protecting a system from data transmission errors.

Receive, Receiver - The process or device assigned to receive messages in a data communications network, usually, but not always, at a DTE device.

Receive Only (RO) - A device capable of receiving data transmissions, but unable to transmit, such as a printer.

Record Separator (RS) - A control character.

Recovery - The procedure or process required to be performed to restore a computer system to a predetermined level of operation or availability after a failure.

Redundancy - A design procedure that uses more system elements than are absolutely necessary to realize all of the systems functions. In data communications, the application of error-detection and correction codes, (software), as well as duplicate FEP 's, communication control units (CCU's), and data channels (hardware) have resulted in an increased percentage of application availability.

Redundancy Check - An error detection process based on the systematic insertion of correction components or characters.

Redundant Code - A code that uses more signal units than needed to represent transmit ted information.

Reference Pilot - Used in carrier systems to allow the adjustment of carrier transmission signals.

Refresh Rate - The rate at which a CRT image is renewed (usually approx. 60 times per second) for a consistent appearance.

Regional Center - A class 1 central office connecting portions of the telephone system together, with each pair of regional centers having a direct circuit group running from one center to the other.

Reliability - From a quantitative standpoint, reliability is the probability that the system or data communications network will perform its intended function over the stated duration of time in the specified environment for its usage. From a qualitative sense, reliability is closely connected with maintainability, availability, and system security from unauthorized access.

Remote, Remote Access - Accessing a computer system from a location of at least several hundred feet, and sometimes very many miles distant. See remote job entry.

Remote Analog Loopback - A diagnostic test that forms the loop at the analog output of the remote modem's Telco line interface to isolate faults.

Remote Batch - A method of submitting jobs to a computer through a remote terminal.

Remote Channel Loopback - A diagnostic test that forms the loop at the channel side of the remote multiplexor.

Remote Composite Loopback - A diagnostic test that forms the "loop" at the composite or output side of the remote multiplexor.

Remote Digital Loopback - A diagnostic test that forms the "loop" at the DTE side of the remote modem.

Remote Job Entry - The submission of jobs to a central computer from a distant location when the length limits of cable connections between input/output devices are exceeded, in which case the telephone or another common carrier link must be used to bridge the gap.

Remote Processing - Relocating a portion of the host computers processing to an off-site location. The remote computer may be a minicomputer under supervision of the host, and connected via telephone links.

Remote Station - A device attached by a telephone link to a controlling unit.

Repeater - Two definitions exist in normal usage:

1) A device used for signal shape and level restoration, for signals that have been distorted due to attenuation .

2) A device used to repeat signals from one circuit onto another circuit (s) usually in a reshaped / amplified form.

Repeater, Telegraph - The device used to accept a telegraph signal, and repeat the same signal for further distant transmission.

Residual Error Rate - A ratio of the number of bits, blocks, characters, etc. incorrectly receive d and undetected/uncorrected to the total number of transmitted bits, blocks, characters, etc.

Resource Class - A term used in a LAN environment to identify a group of computer or computer ports offering similar facilities such as an application program, and identified by a symbolic name.

Response Time - Response time is essentially the elapsed time between an event, and the computer systems response to the event, or, from the final character of a message at the terminal until the receipt of the first character of the reply.

Retransmissive Start - A component used in fiber optic transmission that permits the light signal on input fiber to be retransmitted on multiple output fibers.

Retry - Re transmitting a block, field, or other unit of data a predefined number of times.

Return To Zero (RZ) - The opposite of NRZ, whereby the voltage levels return to zero after each encoded bit. Contrast with NRZ.

Reverse Channel - A method of modem design, also known as "backward channel" whereby a two-wire channel would be used to provide simultaneous communication between the receiver and transmitter. Reverse channel would be used for error control, diagnostics, circuit assurance and circuit breaking.

Reverse Interrupt (RV) - A receiver generated control character sent to request termination of an in-progress transmission.

Ring Indicate, Ring Indicator (RI) - An interface signal defined in RS-232 sent from the modem to the DTE on pin 22 indicating the presence of an incoming call.

S

Satellite Microwave Radio - A communications satellite oriented microwave or beam radio system.

SBS (Satellite Business Systems) - A domestic (U.S.A.) satellite carrier.

Scattering - The signal loss occurring in fiber optic transmission due to light diffusion from variations in the fiber medium.

SDLC (Synchronous Data Link Control) - A communications protocol used in the IBM SNA environment to control, check, initiate and terminate information sessions on transmission lines.

Sectional Center - A class 2 telephone central office in the DDD network. Compare with regional center.

Security - Any method or technique designed to prevent unauthorized physical access to information. Wiretapping or electromagnetic eavesdropping is a security threat whenever data travels through the air

or over wires that are not in a secure area. Most data communication networks use common carrier facilities, and this presents problems. Sensitive data that is to be transmit ted from one location to another should be encrypted to make it private. Privacy transformations involving static methods of coding require a certain amount of work to break, but can usually be decoded after some effort. The best coding techniques involve keys that are as long as the data to be encrypted. By using different starting values, and different related sequences of random numbers, it becomes very difficult to determine the generating algorithm from eavesdropping, so the required work to break the code is very extensive.

Selection - The process of addressing a terminal or printer on a selective calling circuit.

Selective Calling - The process of a master terminal or station selectively choosing the terminal or printer, etc. that would be the recipient of a message.

Selector Channel - A data channel designed to operate with only one input/output peripheral device at a time, at a rate of only one byte at a time, until the complete record is transferred. Contrast with block multiplexor channel and multiplexor channel.

Selector Light pen, Light pen - An input device in the form of a "pen" attached to the display station (CRT) as an extra feature. The lightpen may be pointed at an item on the screen and then activated, thereby selecting the item for subsequent processing.

Self-Checking Numbers - Any numbers containing redundant information to enable error detection.

Serial Transmission - A "normal" mode of information transfer in data communications in which the bits comprising a character are sent in sequence, one at a time. Contrast with parallel transmission, normally used between a computer and its peripherals.

Serving Area - A telephone company’s geographic service area, usually the same as a LATA.

Session - A term used in IBM SNA environment to define the logical link-up between two stations allowing them to communicate.

Session Layer - The fifth layer of the OSI model that addresses establishing, managing, and terminating connections for individual application programs, and interfacing with the transport layer.

Shannon's Law - A formula devised by communications pioneer, Claude E. Shannon. According to Shannon, the maximum amount of information that can be transmitted is twice the frequency of the transmitted signal.

Shared Access - A term used in a LAN environment to describe an access method that allows many terminals to share a transmission medium, as opposed to discrete access . Examples of shared access methods would be explicit access and contended access.

Shielding - The protective coating or shield used on data communications medium, such as coaxial cable.

Shift - See figures shift and letters shift.

Short-Haul - Transmission distances, usually less than 50 miles. Short-Haul Modem (SHM). See line driver.

Sideband - A mode of analog modulation that uses a frequency band on either the upper or lower side of the carrier frequency.

Signal Converter - A device designed to accept input signals in one form and transmit output signals in a different form. See modem.

Signal-To-Noise Ratio (S/N) - The ratio of the relative power levels of a voice/data communications signal and the noise on a line, expressed in decibels (dB).

Sign-On Character - The first character transmit ted on an auto baud circuit to ascertain the data rate.

Simplex, Simplex Circuit - Two definitions exist in normal usage:

1) The transmission of signals in one direction only.

2) A circuit allowing transmission of signals in either direction, but not both directions simultaneously, according to the CCITT.

Simplex Mode - Data communications in only one direction, with no capability for reversing transmission.

Simulation - The employment of the computation process to implement a model of some dynamic system or phenomenon. A number of digital simulation programming languages are available for both mainframe and personal computers alike.

Sine Wave - A continuously variable and repeating signal, discovered by a man named Fourier. A sine wave signal is often used as the carrier in an analog modulation process, as well as being able to represent data via frequency and phase modulation. Sine waves can be generated by electronic oscillators and electromechanical generators.

Single-Mode - A process of using only one "ray" or mode on a fiber optic medium having a core diameter only a few times the wavelength of the transmitted light. The advantage of single mode propagation is to avoid the destructive interference between rays propagated under a different process known as multimode fiber.

Sink - The receiver of a message sent from the source or sender/ transmitter. Contrast with source.

Skewing - The time delay between two data signals.

Sky net - An AT&T communications product offering digital transmission service featuring on-site earth station facilities for wideband satellite transmission using Accunet Reserved 1.5 circuits.

Slave Station - A terminal or other data unit controlled by the master station/ terminal in a point-to-point circuit .

Slicing Level - The voltage threshold determining where a one or a zero bit signal can be distinguished.

Slot - A time unit used in a TDM frame where a sub-channel character or bit is carried to the other end of the circuit and extract **Zero Code Suppression** - The practice of suppressing the transmission of eight of more consecutive binary "0" bits by inserting a binary "1" bit. Zero code suppression is used with digital T1 and related communications facilities.

Zero Insertion - A practice used in an SDLC environment that includes a binary "0" in a stream of transmitted data to avoid confusing SYN characters with data characters. The receiving end removes the inserted zeros.

Zero Transmission Level Point - A point of reference (0 TLP) used to measure signal power gain/loss of a data circuit.

ed by the sink TDM unit.

Slow-Release Relay - An electromechanical relay with a copper sleeve over one end of its core, causing it to be slow in releasing.

Smart Terminal - A data terminal having both communications capabilities as well as local processing capabilities.

SMRT (Single Message-unit Rate Timing) - A message unit system tariff used by telephone companies to measure and time calls in increments of 5 minutes or less, applying a single message unit charge to each increment.

S/N - See signal-to-noise ratio.

SNA (Systems Network Architecture) - An IBM system product offering the computer user a total data processing and data communications system for IBM software and hardware devices. End users are unaffected and independent of the specific data communications system services. SNA 's system functions are separated into three discrete areas: application layer, functional management layer, and transmission subsystem layer.

Soft Copy - A term used to describe a video display image or CRT display offering no provision for a permanent record, such as a printed hardcopy of the display.

T

Table Driven - A data communications process that uses table lookup to route messages in a network, operate a modem or provide data security access.

Tail Circuit - A term used to describe a circuit type (usually a dedicated line) that feeds data to a network node.

Tandem Data Circuit - A data circuit designed to connect two DCE devices in series.

Tap - A term used in a LAN environment to describe the connection to the main transmission medium.

Tariff - Basically, a contract between the customer (subscriber)and common carrier, through which regulating agencies approve or disapprove such facilities or services. A tariff is very specific regarding service rates, types of services provided, facilities, etc.

TASI (Time Assignment Speech Interpolation) - A method of activating data communication channels via speech. Other application signals may be multiplexed on the same circuit when speech is not present, thereby achieving line efficiency.

TC (Transmission Control) - A control character grouping, also known as "telecommunications control" or "technical control".

TCAM (Telecommunications Access Method) - An IBM data communications software routine designed to facilitate and control the transfer of messages between the application program and the remote 3270 terminals.

TCP/IP (Transmission Control Protocol/Internet Protocol) - A communications protocol, functioning within the third and fourth OSI layers, used in a LAN environment for internetwork routing and reliable message delivery. TCP/IP is found in ARPANET and is endorsed by the DOD.

TCU (Transmission Control Unit) - A controller whose functions are dependent upon a stored program of instructions from the host computing system. A TCU (IBM 2703, for example) is therefore unlike a communications control unit which has the ability to execute its own stored program.

TD (Transmit Data) - The RS 232 data signal sent on pin 2 from a DTE device to a DCE device.

TDM (Time Division Multiplexer) - A multiplexer designed to apportion its composite link time between its available channels, interleaving data at a higher speed on the main or multiplexed channel . The data signals are then separated to restore the data to the individual input channels.

TDMA (Time Division Multiple Access) - A mode of operation used in both satellite communication as well as LAN environments. TDMA utilizes a high speed, burst mode of operation to interconnect LAN 's, while it is also used to allow several earth stations to "timeshare" satellite transponder bandwidths.

Telco - A term used to represent "telephone company", in the United States.

Telecommunications - The transmission (and reception) of signals producing sounds, images or information using a variety of media such as fiber optic, copper wire, infrared or radio frequency.

Teleconferencing - Engaging in a conference between remote stations linked by a telecommunications medium.

Telecopy - A facsimile device designed to transmit documents to a remote location via a data communications line.

Telegraphy - A method of data communications using 75 bps as a transmission speed.

Telemetry - The process of transmitting and collecting coded, analog data, often realtime parameters, from a remote environment.

Telnet - A proprietary term for a VAN service provided by the GTE Telenet Corporation.

Telephony - A term initially used to describe voice telecommunications, but now used to describe voice/data/video communications.

Tele printer - A term used to describe various types of terminals consisting of both keyboard and printer but no CRT.

Teleprocessing - A term that is synonymous with data communications, indicating any data processing system that uses communications facilities. The word "teleprocessing" once was an IBM trademark.

Teletype, Teletype Corporation - A trademark (and manufacturer) for a series of different types of teleprompter equipment designed for data communications systems.

Teletypewriter Exchange Service (TWX) - A data communications service provided by the AT&T Corporation using teletypewriter stations connected to phone lines, for access to other TWX stations. TWX supports both ASCII and Baud coded machines.

Telex Service - A data communications service using dial-up lines and Baudot code, allowing customers to communicate temporarily and directly between themselves, using asynchronous apparatus and the circuits of the public telegraph network, world wide. Computers may be connected to the Telex network.

Terminal - A device designed to allow users of a data processing system to gain access to information in a more conventional manner than through the input/output devices local to that system. Often, computer terminals are located away from the host, at locations convenient to the users.

Terminal Control Unit, Terminal Controller - See cluster control unit.

Terminal Node - A term used in IBM SNA environment to describe a non user-programmable peripheral node.

Terminal Polling - See polling.

Terminal Server - A device used in an Ethernet LAN environment allowing one or more devices to be connected to the Ethernet network.

Test Center - A designated installation used to diagnose problems with data communications lines and equipment. Test centers are often combined with installations performing network control.

Test Mode - A modem or DSU status that disables both transmitter and receiver in order to perform a test in progress of the line.

Throughput - The average rate at which jobs are completed by the system in an interval of time or the rate at which information is communicated during a specified time period. Throughput is frequently used as a figure of merit for a system, so that the higher the throughput, the more highly regarded the system is, but some factors must also be considered or throughput will be deceptive. The capacity of the system, the time interval over which the throughput is measured, the load on the system the scheduling method, and the job mix all act as factors that have an affect on system/ data communications throughput.

Throughput Delay - The amount of time needed to accept data input and transmit is as output.

Tie Line - A service of telephone common carriers offering a private line that connects two or more points together.

Timed Release Circuit - A type of circuit designed to automatically release other connected circuits after a preset interval.

Timing - The setting and observing of the elapsed time of an action or data communications process, often the function of a modem.

Timeout - A method used to improve and minimize user response times by allocating a terminal or other computer device for a predefined time period, after which if no activity is present on the terminal session or connection is terminated.

Timesharing, Time Sharing - A method of operating a computer so that two or more users are simultaneously able to present problems to the machine and retrieve information from it usually by doing some computation of processing for one user, putting it aside, then doing some computation for a different user. A clocking mechanism would send the CPU interrupts at a predefined interval to provide a timesharing environment for connected terminals.

Time Slot - A term used in a LAN environment to describe a sequence position or assigned time period.

TNC (Threaded-Neill-Councilman) - A type of miniature coaxial cable connector using a threaded connector instead of a bayonet lock connector.

Token, Token Passing - A term used in a LAN environment to describe the special "message" called a token, that allows a station to control the transmission medium. The token is transmit ted from node to node. When the receiving station is in possession of the token, it may transmit messages before passing the token on to the next node. See token bus, token ring.

Token Bus - A LAN environment bus topology using a token for explicit access and all stations attached to the bus listen for the token. A station must first receive the token before transmitting. Contrast with token ring.

Token Ring - A LAN environment topology that uses a token for explicit access. Unlike token bus, the token is passed from station to station, in sequential order, so that the next logical station that receives the token will also be the next physical location.

Toll Center - A Class 4 central office which terminates message circuits and channels.

T-1 Timer - A term used in packet-switched network environments to measure the interval of timeouts during data exchanges and link initialization.

Topology - The arrangement of stations and the links connecting the stations of a data communications network. See network topology.

Touch-Tone - An AT&T proprietary trademark for push-button, DTMF dialing method.

Traffic - The quantity and movement of messages through a data communications system.

Traffic Engineering - The science of communications facility design and optimization to provide for maximum user/ application availability.

Trailer Block, Trace Block - Control information used for timing, error correction and recovery, etc., that follows the message text

U

UART (Universal Asynchronous Receiver/Transmitter) - A microchip device performing asynchronous communication functions by converting parallel digital output from a DTE device into bit serial transmission (and bit serial into parallel).

UHF (Ultra High Frequency) - The range of frequencies, spanning between 300 mHz and 3 gHz, used for cellular radio frequencies (RF) and for UHF television channels 14 through 83).

ULSI (Ultra Large Scale Integration) - A term describing an ultra- high density microchip containing over 10,000 circuits.

Unattended Mode, Unattended Operations - A term used to describe an automatically operating communications device, such as an auto- answer modem.

Unbalanced, Unbalanced To Ground - A term used to describe the condition present in a two wire circuit when the impedance-to- ground on one wire is different from that of the other. Contrast with balanced, balanced-to-ground.

Unbundling - A term used to describe the itemization of common carrier or vendor provided communications services.

Uncontrolled Terminal - A computer terminal containing no polling or control logic and is always online to the CPU.

Uninet - A data communications common carrier offering an X.25 PDN.

UNIX - An AT&T proprietary operating system designed for multi- user, multi-tasking data communications operating systems.

UPC (Universal Product Code) - The "bar code" used to identify consumer and industrial products in mechanized inventory systems.

Up-Link - A term used in satellite communications to describe the earth station and the transmit ted signal to a communications satellite . Contrast with down-link.

Uptime - The period of time that a computer application or data communications link would be available to the user community on an underrated, and uninterrupted basis. Contrast with downtime.

Upward Compatible - An application program having the characteristics of compatibility with an enhanced mode or operation (such as a newer release or version operating system).

USART (Universal Synchronous/Asynchronous Receiver/Transmitter) - A semiconductor device performing synchronous/asynchronous conversion from a communications processor to the correct format for data transmission.

USASCII (United States of America Standard Code for Information Interchange) - See ASCII.

USRT (Universal Synchronous Receiver/Transmitter) - A semiconductor device that formats data for communications over a synchronous data circuit.

Utility, Utility Program - A computer program designed to perform a task required by many or most of the computing systems users, the most common of which are those that copy information from one medium to another and those used to streamline an operation.

V

Validity, Validity Checking - The practice and techniques of error checking after data has reached its destination.

Value Added Carrier - A common carrier or communications vendor that provides an enhanced service to a data communications circuit.

VAN (Value Added Network) - A leased network provided by a common carrier or vendor that has been enhanced with extra computer equipment to provide more services. Many PDN's also are VAN's.

Vertical Parity, Character Parity - One of many different forms of error detection using a vertical parity count within the bits of each character transmitted. If any error is found, the character or block of characters would be re transmit ted, with the amount of re transmission dependent upon the computing system.

Vertical Redundancy Check (VRC) - A method of error detection using an extra bit, called a parity bit, in each character for checking purposes. The receiving station detects whether there is an odd number of 1's or even (depending on whether the system uses even or odd parity). Noise or distortion on the line may have caused a bit to be lost or added. The error is either noted or the receiving station may instigate are transmission.

VF (Voice Frequency) - Sometimes referred to as "voice grade frequency", VF represents the 4.2 kHz bandwidth telephone circuit used for voice transmission.

VHF (Very High Frequency) - A term used to describe a radio carrier frequency band ranging from 30 MHz to 300 MHz

Video Conferencing - A method of audio/video communications, usually employing satellite transmission over a wideband range spanning between 56 kbps to 1.544 mbps (T1 circuit speed).

Virtual - At least two applications of the term "virtual" are commonly used in data communications:

1) A term generally used to describe the main memory of a virtual (simulated) computer. Using virtual memory, via address space, memory space and address translation/mapping, greater memory capacity is possible and faster processing can occur because only that portion of a program needed at the moment is drawn into memory. The programmer can be confident of highly efficient operation of the program.

2) From a data communications standpoint, the term virtual has a similar connotation, implying infinite capacity of data channels and circuits.

Virtual Circuit - A data circuit that exists only for the duration of a call, but is sharing a data channel with other calls on virtual circuits.

VLF (Very Low Frequency) - A term used to describe a radio carrier frequency band ranging from 3 kHz to 30 kHz.

VLSI (Very Large Scale Integration) - A term used to describe a very high density microchip containing up to 10,000 circuits.

Voice band - A voice grade bandwidth typically spanning between 300 and 3300 Hz.

Voice/Data PABX - A user owned, automatic telephone exchange combining the functions of a voice PABX and a data PABX, sometimes used for DOV services.

Voice Digitizing - The process of converting an analog voice signal into digital signals for transmission.

Voice Grade Channel - See channel, voice grade.

Volatile - A memory device type that loses its stored contents upon electrical power fluctuation or failure.

VRC - See vertical redundancy check and parity check.

VTAM (Virtual Telecommunications Access Method) - An IBM software routine providing users of 3270 type remote terminal systems access to applications programs while using the data communications network cost effectively.

W

WACK/WAK (Wait Acknowledge) - A signal sent to a transmit ting station indicating the receiving station is temporarily unable to receive data.

WAN (Wide Area Network) - A term used to describe a data communications network using common carrier circuits to connect stations and processors. Contrast with LAN.

WATS (Wide Area Telephone Service) - A type of long distance telephone service characterized by calls measured on a bulk rate basis. WATS uses a zone system whereby a customer may make outgoing calls or receive incoming calls (INWATS) and be charged based on the specific zones involved.

Waveguide - A term used in a microwave communications environment to describe a hollow metallic media used for data transmission.

Wavelength - Refers to the distance between the successive peaks of a sine wave.

WESTAR - The Western Union Co.'s data communications satellites. White Noise -See Gaussian noise.

Wide Band - See broadband.

Window - A term used to describe the amount of data (packets, messages, etc.) that may be transmit ted to a receiver before a reversal of transmission direction.

Wiring Closet - A point of termination for telephone equipment, usually located at a customer's premises, providing access for telephone repair personnel.

Wire Center - A centralized location of wires from subscribing stations, located to provide efficient and economical distribution of wires and cables. The central office is usually located at the wire center of the subscribing telephones in order to efficiently use the exchange outside the plant.

Wire Pairs - A method of transmission using a circuit composed of two (normally copper) wires.

Word - The sequence of either bits or characters capable of being stored and processed as a unit.

Word Length - The number of bits in a word, usually based on the internal operation of a computer, such as 8, 16, 24 and 32 bit CPU 's.

Workstation - The terminal or other device, at which a computer operator works, capable of sending and receiving data needed to perform a specific task. An Input/output terminal .

WPM (Words per Minute) - A term used in the telegraph environment to measure transmission speed.

X

Xerox - The Corporation credited as the originator of Ethernet.

XMODEM - A communications protocol devised by Ward Christiansen to perform simple error checking between microcomputers. XMODEM is a half-duplex protocol, used on full-duplex circuits transmitting 128 characters per block. After information is sent, the sender waits for a reply before transmitting the next message.

XNS/ITP (Xerox Network Systems'/Internet Transport Protocol) - A communications protocol used in a LAN environment between networks, functioning similar to the TCP/IP.

Y

YMODEM - A communications protocol very similar to XMODEM designed to perform simple error checking between microcomputers. YMODEM is a half-duplex protocol, used on full-duplex circuits transmitting a 1 kilobyte (1,024) characters per block. After information is sent, the sender waits for a reply before transmitting the next message

Z

Zero Code Suppression - The practice of suppressing the transmission of eight of more consecutive binary "0" bits by inserting a binary "1" bit. Zero code suppression is used with digital T1 and related communications facilities.

Zero Insertion - A practice used in an SDLC environment that includes a binary "0" in a stream of transmitted data to avoid confusing SYN characters with data characters. The receiving end removes the inserted zeros.

Zero Transmission Level Point - A point of reference (0 TLP) used to measure signal power gain/loss of a data circuit.