Networking Technologies

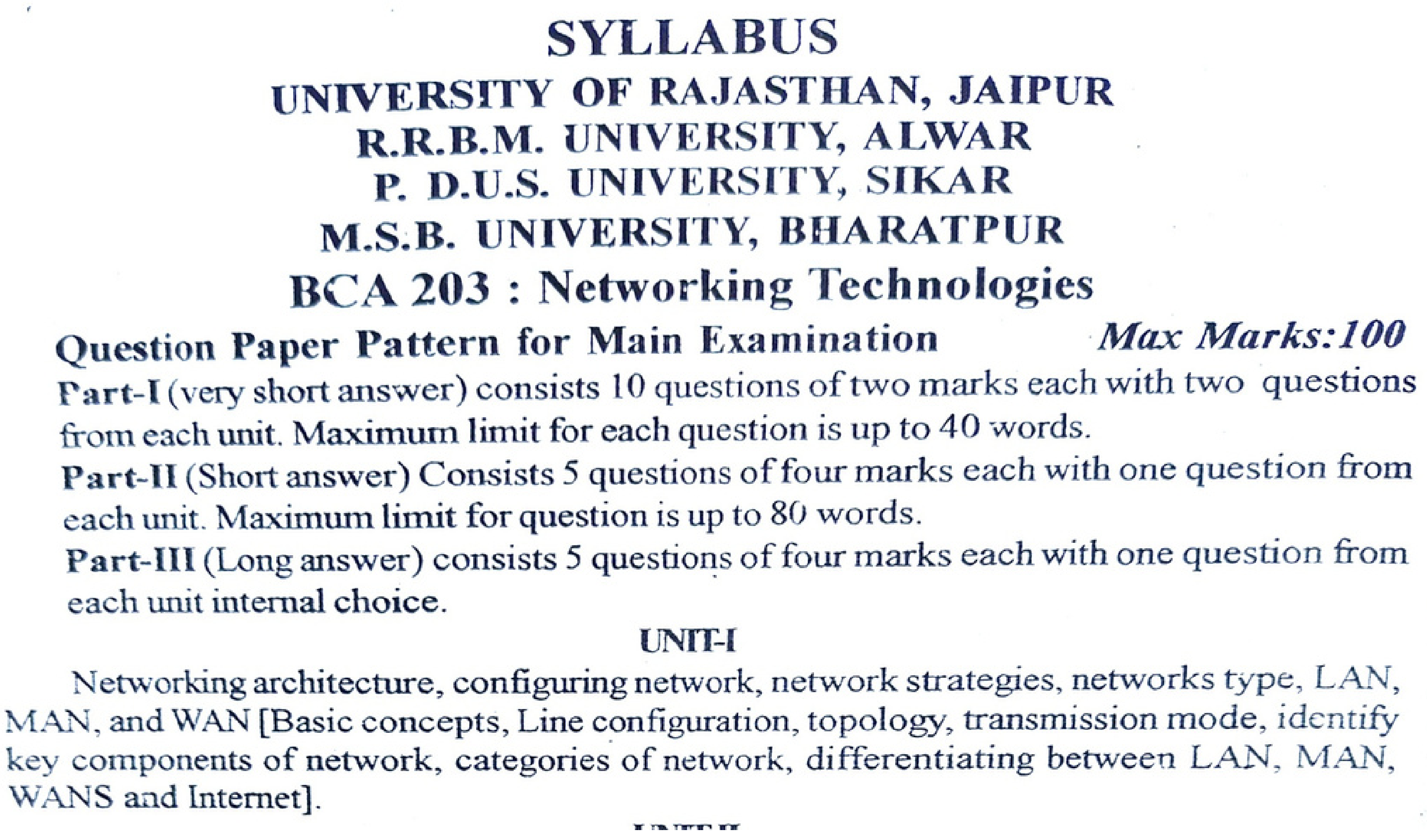
[As per latest Syllabus of University of Rajasthan, ***Jaipur,*** *R.R.B.M. University,* ***Alwar****, P.D.U.S. University,* ***Sikar*** *and M.S.B. University,* ***Bharatpur*** *for B.C.A.Part-III]*

BCA -303

Author

Kajali Jain
Lecturer,
Compucom Institute of Technology
and Management, Jaipur

New Edition
2019



SYLLABUS

UNIVERSITY OF RAJASTHAN, JAIPUR
R.R.B.M. UNIVERSITY, ALWAR
P. D.U.S. UNIVERSITY, SIKAR
M.S.B. UNIVERSITY, BHARATPUR
BCA 203 : Networking Technologies

Question Paper Pattern for Main Examination ***Max Marks:100***

Part-I (very short answer) consists 10 questions of two marks each with two questions from each unit. Maximum limit for each question is up to 40 words.

Part-II (Short answer) Consists 5 questions of four marks each with one question from each unit. Maximum limit for question is up to 80 words.

Part-III (Long answer) consists 5 questions of four marks each with one question from each unit internal choice.

UNIT-I

Networking architecture, configuring network, network strategies, networks type, LAN, MAN, and WAN [Basic concepts, Line configuration, topology, transmission mode, identify key components of network, categories of network, differentiating between LAN, MAN, WANS and Internet].

UNIT-II

Chapter

1

Computer Networking-An Overview

1.0 Introduction

Data Communication and networking are changing the way we do business and the way we live. Business decisions have to be made ever more quickely and the decision makers require immediate access to accurate information. Why we wait for a week for that report from Germany to arrive by mail when it could appear almost instantaneousely through computer networks ?

What is computer network ? A computer network is a collection of computers inter connected by one or more transmission paths. The transmission path often is the telephone line, due to its convenience and universal presence. The network exist to meet one goal; the transfer and exchange of data between the computers and terminals.

The development of-the personal computer brought about tremendous changes for business, industry, science and education. A similar revolution is occuring in data communications and networking. Technological advances are making it possible for communication links to carry more and faster signals. As a result, services are evolving to allow use of his expanded capacity. For example established telephone services such as conference calling, call waiting, voice mail. and called ID have been extended.

Research in data communications and networking has resulted in new technologies. One goal is to be able to exchange data such as text, audio and video from all points in the world. We want to access the Internet to download and upload information quickly and accurately and at any time.

This chapter addresses four issues : data communications, networks, the internet and protocols and standard. First we give a broad definition of data communications. Than we define networks as a highway on which data can travel. The internet is discussed as a good example of an internetwork (i.e. a network of networks). Finally, we discuss different types of protocols, the difference between protocols and standards and the organization that set those standards.

1.1 Data Communications

When we communicate, we are sharing informations. This sharing can be local or remote. Betwen individuals, local communication usually occurs face to face, while remote communication takes place over distance. The term telecommunication, which includes telephony, telegraphy, and television, means communication at a distance (tele is Greek for "far").

The word data refers to information presented in whatever from is agreed upon by the particles creating and using the data.

Data communications are the exchange of data between two devices via some from transmission medium, such as a wire cable. For data communicaitons to occur, the communicating devices must be part of a communications system made up of a combination of hardware (physical equipment) and software (programs). The effectiveness of a data communications system depends on four fundamental characteristics : delivery, accuracy, timelines and filter.

1. **Delivery :** The system must deliver data to the correct destination. Data must be received by the intended device or user and only by that device or user.
2. **Accuracy :** The system must deliver the data accurately. Data that have been altered in transmission and left uncorrected and insolvable.
3. **Timelines :** The system must deliver data in timely manner. Data delivered late are useless. In the case of video and audio, timely delivery means delivering ata as they are produced, in the same order that they are produced, and without significant delay. The kind of delivery is called real-time transmission.
4. **Filter :** Filter refers to the variation in the packet arrival time. It is the uneven delay in the delivery of audio or video packets. For example, let us assume that video packets are sent every 30 ms. It some of the packets arrive with 30 ms delay and offer with 40 ms delay, an uneven quality in the video is the result.

Components

A data communications system has five components.

1. **Message :** The message is the information (data) to be communicated. Popular forms of information include text, numbers, pictures, audio and video.
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 receives the message. It can be a computer, workstation, telephone handset, television and so on.
4. **Transmission medium :** It is the physical path by which a message travels from sender to receiver. Some examples, of transmission media include twisted-pair wire, coaxial cable, fibre-optic cable and radio waves.

5. **Protocol :** A protocol is a set of rules that govern data communications. It represents an aggreement between the communicating devices. Without a protocol, two devices may be connected but not. Communating, just as a person speaking French cannot be understand by a person who speaks only Japanese.

1.2 Data Representation

Information today comes in different forms such text, numbers, images, audio and video.

- **Text :** In data communication, text is represented as a bit pattern, a sequence of bits (0's or 1s). Different sets of bit patterns have been designed to represent text symbols. Each set is called a code, and the process of representing symbols is called coding. Today, the preventing coding system is calleld unicode, which uses 32 bits to represent a symbol or character used in any language in the world. The Americal Standard Code for Informaiton Interchange (ASCII), developed some decades ago in the united states, now constitutes the first 127 characters in unicode and is also referred to as Basic Latin.
- **Numbers :** Numbers are also represented by bit patterns. However, a code such as ASCII is not used to represent numbers; the number is directly converted to a binary number to simply mathematical operations.
- **Images :** Images are also represented by Bit patterns.In its simplest form, an image is composed of a matrix of pixels (picture elements), where each pixel is a small dot. The size of the pixel depends on the resolution. For example, an image can be divided into 1000 pixels or 10000 pixels. In second case, there is a better representation of the image (better resolution) but more memory is needed to store the image.

  After an image is divided into pixels, each pixels assigned a bit pattern. The size and the value of the pattern depend on the image. For an image made of only black and white dots (e.g. a chessboard), a 1-bit pattern is enough to represent a pixel.

  If an image is not made of pure white and pure black pixels, you can increase the size of the bit pattern to include grey scale. For example, to show four levels of grey pixel by 01, a light gray pixel by 10 and a white pixel by 11.

  There are several ways to represent colour images. One method is called RGB, so called because each colour is made of a combination of three primary colours : reg, green and blue. The intensity of each colour is measured and a bit pattern is assigned to it. Another is YCM, which is made up of yellow, cyan and magenta.

- **Audio :** Audio refers to the recording or broadcasting of sound or music. Audio is by nature different from text, number or images. It is continuous, not discrete. Even when we use a microphone to change voice or music to an electric signal, we create a continuous signal.
- **Video :** Video refers to the recording or broadcasting of a picture or movie. Video can either be produced as a continuous entity (e.g. by a TV camera), or it can be a combination of image, each a discrete. entity, arranged to convey the idea of motion. Again we can change video to a digital or analog signal.

1.3 Evolution of Computer Networks

Computer Networking of today has its roots in Defence Advanced Research Projects Agency (DARPA) of the USA which sponsored the research in 1960's. The US government played a critical role in the evolution and application of advanced computer networking technology over several decades. Today's computerized communication network are based on a technoiogy called **packet switching,** which is fundamentally different from the technology that was then employed by the telephone system and was based on **circuit switching.**

The ARPANET grew four nodes (computer) in 1969 to roughly one hundred by 1975. During the International Conference on computer Communication in oct 1972, an International Network Working Group (INWG) emerged which went on to develop an international standard for packet communication of commerical packet switching in the USA, Canada, France and the UK.

By mid-1975, DARPA had concluded that the ARPANET was stable and should be turned over to a seperate agency for operational managment.

Responsibility was, therefore transferred to the Defence communication Agency, which is now known as the Defence Information System Agency.

In 1977 a four network demonstration was conducted linking ARPANET, SATNET, ETHERNET and the PRNET. In the early 1970, DARPA intiated research at stanford for designing a new set of computer communication protocols. Protocols are rules and regulation that allow multiple packet network to be interconnected in a flexible and dynamic way, TCP/IP are two main protocols of Internet-Transmission Control Protocol and Internet Protocol.

In the past years, commercially use of the Internet had spread globally. The Internet is growing exponentially in the number of networks hosts and volume of traffic involved. The number of host computer increased from 200 to 5,00,0000 in the first twelve year between 1983 and 1995 and the number of hosts in doubling every year since then.

Computer Telephony

Before the advent of computer networks that were based upon some type of telecommunications system, communication between calculation machines and early computers was performed by human users by carrying instructions between them.

In september 1940 George Stibitz used a teletype machine to send instructions for a problem set from his model K at Dartmouth College in New Hampshire to his Complex Number Calculator in New york and received results back by the same means. Linking output systems like teletypes to computers was an interest at the advanced Research Projects Agency (ARPA) when, in 1962, JCR liklides was hired and developed a working group he called the "Intellectual Network", a precursor to the ARPAnet.

In 1964, researchers at Dartmouth developed the Dartmouth Time sharing system for distributed users of larger computer system. The same year, at MIT, a research group supported by General Electric and Bell Labs used a computer (DEC's PDP 8) to route and manage telephone connections.

Throughout the 1960, Leonard Kleinrock Paul Baran and Donald Davies independently conceptualized and developed network systems, which used datagrams or packets that coul be used in a packet switched network between computer systems.

1965, Thomas Merrill and Lawrence G. Roberts created the first wide area network (WAN). The first widely used PSTN switch that used true computer control was the western Electric 1ESS switch, introduced in 1965.

In 1969, the university of california at los angels SRi (in stanford), University o California at Santa Barbara and the University of Utah were connected as the begining of the ARPANet network using 50 Kbit/s circuits.

Commercially service using X.25, an alternative architecture to the TCP/IP suite, were developed in 1972.

Computer network, and the technologies needed to connect and communicate through and between them, continue to drive computer hardware, software and peripherals industries.

Today, computer networks are the core of modern communication. For example, all modern aspects of the Public Switched Telephone Network (PSTN) core computer controlled and telephony increasingly runs over the Internet Protocal, although not neccessorily the Public Internet. The scope of Communication has increased significantly in the past decade and this boom in communications would not have been possible without the progressively advancing computer network.

Network Architecture :

While designing the network architecture, network may be single homogenears mesh comprised of a single type of node and a single type of link network architecture might be heirarchical network with one type link riding on another. The application might be kept seperate without sharing resources at several levels of the network until, at the highest level, they share common facilities. There a may be uncertainty about the proper network architecture of several alternatives may head to be explored.

Another issue relating to the overall architecture of a network is whether to decompose the network into sub networks for the sake of design and operation. It is possible e.g. to begin by dustering the nodes into regions locate gateways within each region and then design a backh one connecting the gateways. All communication between region via this backone local access networks are designed within each region. This is often the Wan which include lan's are designed.

Configuring Networks

A network must be able to meet a certain numbers of criteria. The most important of these are performance reliability and security.

Performance : Performance can be measured in many ways including transit time and response time. Transit time is the amount of time required for a message to travel from one device to another. Response time is the elapsed time between an enquiry and a response. The performance of a network depends on a number of factors, including the number of users, the type of transmission medium, the capabilities often connected hardware and the efficiency of the software.

Performance is often evaluated by two networking metrices throughput and delay.

Reliability : In addition to accuracy of delivery network reliability is measured by the frequency of failure, the time it takes a link to recover from a failure and the network robustness in a catestrophe.

Security : Network security issues include protecting data from unauthorized access, protecting data from damage and development and implementing policies and procedures for recovery from breaches and data loses.

Network Strategies

A network must satisfy following criteria-

a. Performance : Performance can be measured by transit time (propagation delay) and response time speed of operation. Performance is decided by many factors such as number of users, type of transmission medium, hardware and software.

b. Reliability : A network reliability is measured by accuracy failure rate estabilishment time and robustness.

c. Security : Network security concerned with protection of data from unauthorized access.

1.4 Types of Networks

Today when we speak of networks, we are generally referring to two primary categories; local-area networks and wide-area networks. The category into which a network falls is determined by its size. A LAN normally covers an area less 10 km; a WAN can be worldwide. Networks of a size in between are normally referred to as metriolitan-area networks and span tens of miles.

Local Area Network

A local area network (LAN) is usually privately owned and links the devices in a single office, building, or campus (see Figure 1.10). Depending on the needs of an organization and the type of technology used, a LAN can be as simple as two PCs and a printer in someone's home office; or it can extend throughout a company and include audio and video peripherals. Currently, LAN size is limited to a few kilometers.

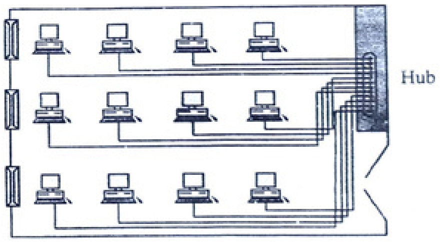


Fig. 1.10 : An isolated LAN connecting 12 computers to a hub in a closet

LANs are designed to allow resources to be shared between personal computers of workstations. The resources to be shared can include hardware (e.g. a printer), software (e.g., an application program), or data. A common example of a LAN, found in many business environments, links a workgroup of task-related computers, for example, engineering workstaions or accounting PCs. One of the computers may be given a large capacity disk drive and may become a server to clients. Software can be stored on this central server and used as needed by the whole group. In this example, the size of the LAN may be determined by licensing restrictions on the number of users per copy of software, or by restrictions on the number of users licensed to access to operating system.

In addition to size, LANs are distinguished from other types of networks by their transmission media and topology. In general, a given LAN will use only one type of transmission medium. The most common LAN topologies are bus, ring, and star.

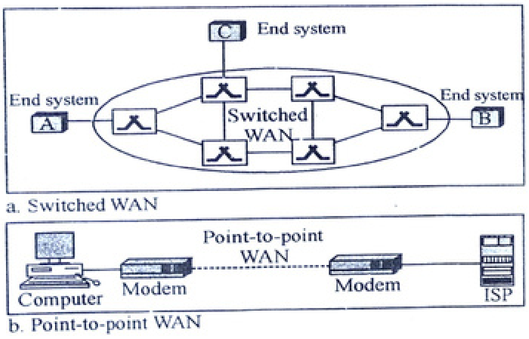
Early LANs had data rates in the 4 to 16 megabits per second (Mbps) range. Today, however, speeds are normally 100 or 1000 Mbps.

Wireless LANs are the newest evolution in LAN technology.

Wide Area Network

A wide area network (WAN) provides long distance transmission of data, image, audio, and video information over large geographic aras that may comprise a country, a continent, or even the whole world. A WAN can be as complex as the backbones that connect the Internet or as simple as a dial up line that connects a home computer to the Internet. We normally refer to the first as a switched WAN and to the second as a point to point WAN (Figure 1.11). The switched WAN connects the end systems, which usually comprise a router (internet working connecting device) that connects to another LAN or WAN. The point to point

WAN is normally a line leased from a telephone or cable TV provider that connects a home computer or a small LAN to an Internet service provider (ISP). This type of WAN is often to provide Internet access.



a. Switched WAN

b. Point-to-point WAN

Fig. 1.11 : WANs a switched WAN and a point-to-point WAN

An early example of a switched WAN is X.25, a network designed to provide connectivity between end users. X.25 is being gradually replaced by a high speed, more efficient network called Frame Relay. A good example of a switched WAN is the asynchronous transfer mode (ATM) network, which is a network with fixed-size data unit packets called cells. Another example of WANs is the wireless WAN that is becoming more and more popular.

Metropolitan Area Networks

A metropolitan area network (MAN) is a network with a size between a LAN and a WAN. It normally covers the area inside a town or a city. It is designed for customers who need a high speed connectivity, normally to the Internet, and have endpoints spread over a city or part of city. A good example of a MAN is the part of the telephone company network that can provde a high speed DSL line to the customer. Another example is the cable TV network that originally was designed for cable TV, but today can also be used for high speed data connection to the Internet.

1.5 Interconnection of Networks : Internetwork

Today, it is very rare to see a LAN, a MAN, or a LAN in isolation; they are connected to one another. When two or more networks are connected, they become an internetwork, or internet.

As an example, assume that an organization has two offices, one on the east coast and the other one the west coast. The established office on the west coast has a bus topology LAN; the newly opened office on the east coast has a star topology LAN. The president of the company lives somewhere in the middle and needs to have control over the company from her home. To create a backbone WAN for connecting these three entities (two LANs and the president's computer), a switched WAN (operated by a service provider such as a telecom company) has been leased. To connect the LANs to this switched WAN, however, three point-to-point WANs are required. These point-to-point WANs can be a high-speed DSL line offered by a telephone company or a cable modem line offered by a cable TV provider as shown in Figure 1.12.

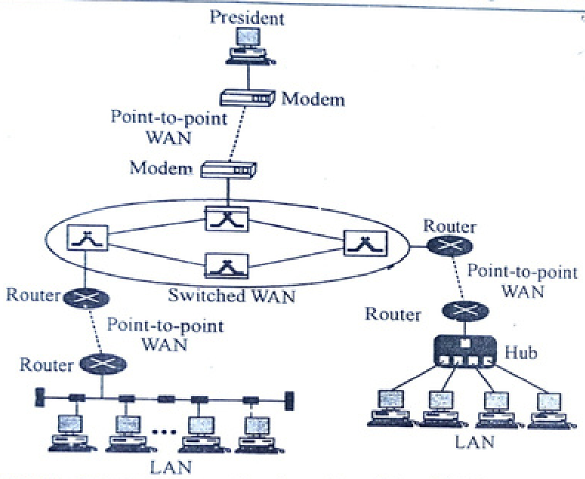


Fig. 1.12 : A heterogeneous network made of four WANs and two LANs

Line configuration :

Line coding is the process of converting bit stream into digital signal fig. 1 shows the process of line coding.

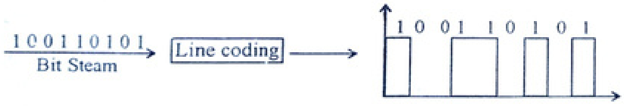


Fig. 1 Line coding

Characteristic of line coding

(a) Signal level versus data level :

1. The number of values allowed in a signal is reforred as number of signal levels and number of values used to represent data as number of data levels.

2. Consider the signal shown in Fig. 2

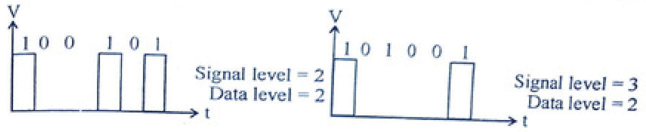


Fig. 2 Signal level versus data level

(b) Pulse Rate Versus Bit Rate

1. Pulse rate is number of pulses per second. Bit rate is a number of bits per second.

$$\boxed{\text{Bit rate} = \text{Pulse rate} \times \log_2 L}$$

where

Lis number of data levels of the signal.

(c) D.C. Components-

1. D.C. components cannot pass through transformers.

2. It is extra energy component.

Fig. 3 shows two signals, with, and without d.c. components

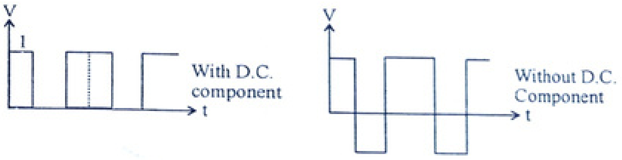


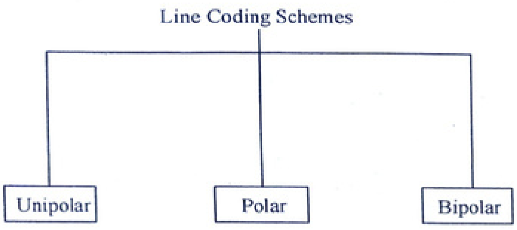
Fig. 3 D.C. Component

4. Self synchronization

There is enough timing information in the transmitted data that keeps sneder and reciever synchronized. This feature is called as self synchronization digital signal.

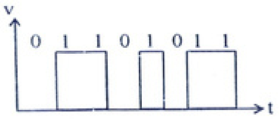
Line coding schemes

The line coding schemes can be categorized into three types-unipolar polar bipolar



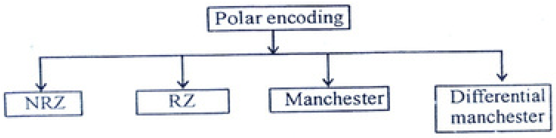
Line coding Schemes

Unipolar : Unipolar encoding uses only one voltage level 1's are encoded as positive value and 0's are encoded as zero value fig. shows unipolar encoding.



Unipolar encoding

2. Polar



Polar encoding types

Polar encoding uses two voltage levels, positive and negative. There are four types of commonly used polar encoding schemes NRZ, RZ Manchester, Differential manchester Fig. 3 shows polar encoding types.

- Non Return to Zero (NRZ) encoding user either positive or negative signal. In NRZ-L (NRZ-level) encoding the level of signal depends on the type of bit that it represents. In NRZ-I (NRZ-Invert), the signal is inverted if a '1' is encountered.
- Return to Zero (RZ) uss three values, positive negative and zero. The RZ encoding provides syncronization information.

- Manchester Encoding uses an inversion at the middle of each bit interval for synchronization and bit representation.
- Differential Manchester uses the inversion at middle of bit interval for synchronization purpose. The bit representation is defined by the inversion or noninversion at the begining of the bit.

Bipolar

- Bipolar encoding user three levels positive zero and negative. Zero level represent binary '0' and alternoting positive and negative voltages represents binary '1'. An example of bipolar encoding is alternate mark Inversion (AMI).

Networks

A network is a set of devices (often refered to as nodes) connected by communication links. A node can computer, printer or any other device capable of sending and/or receiving data generated by other words on the network.

Distributed processing

Most networks use distributed processing, in which a task is divided among multiple computers. Instead of one single large machine being responsible for all aspects of a process, separate computers' (usually a personal computer or workstaion) handle a subset.

Network Criteria

A network must be able to meet a certain number of criteria. The most important of these are performance, reliability and security.

Performance

Performance can be measured in many ways, including transit time and response time. Transmit time in the amount of time required for of message to travel from one device to another. Response time is the claped time between any inquiry and a response. The performance of a network depends on a number of factors including the number of users, the type of transmission medium, the capabilities of the connected hardware, and efficiency of the software.

Performance is often evaluated by two networking matrix : throughput and delay. We often need more throughput and less delay. However, these criteria are often contradictory. If we try to send more data to network, we may increase throughput but we increase the delay because of the traffic congestion in the network.

Reliability

In addition to accuracy of delivery, a network reliability is measured by the frequency of failure, the time it takes a link two recover from a failure, and the network robustness in a catastrophe.

Security

Network security issue included protecting data from unathorised access, protecting data from damage and development and implementing policies and procedures for recovery from breaches and data losses.

1.6 Physical structures

We define some networks :

Type of connection :

A network is two or more devices connected through links. A link is a communications pathway that transfers data from one device to another. for visualization purposes, it is simplest to imagine any link as a line drawn between two points. For communiation to occur, two devices must be connected in some way to same link at the same time.

There are possible types of connections : points to point and multipoint.

Point-to-point : A point-to-point connection provides a dedicated link between two devices. The entire capacity of the link is reserved for transmission between those two devices. Most point to point connection use an actual length of wire or cable to connect the two ends.

Multipoint : A multipoint (a.k.a. multidrop) connection is one which more than two specific devices share a single link.

In a multipoint environment, the capacity of the channel is shared, either spccially or temporally. If several devices can use the link simultaneously, it is a spccially shared connection. If uses's must take turns, it is a timeshared connection.

1.7 Topologies

Type of Connection

A network is two or more devices connected through links. A link is communications pathway that transfers data from one device to another. For visualization purposes, it is simplest to imagine any link as a line drawn between two points. For communication to occur, two devices must be connected in some way to the same link at the same time. There are two possible types of connections, point to point and multipoint.

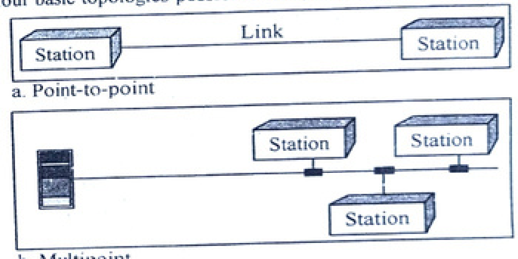
Point-to-point (A point-to-point connection provides a dedicated link between two devices. The entire capacity of the link is reserved for transmission between those two devices. Most point-to-point connections use an actual length of wire or cable to connect the two ends) but other options, such as microwave or satellite links, are also possible (see Figure 1.3a). When you change television channels by infrared remote control, you are establishing a point-to-point connection between the remote control and the television's control system.

Multipoint A multipoint (also called multidrop) connection is one in which more than two specific devices share a single link (see Figure. 1.3b).

In a multipoint environment, the capacity of the channel is shared, either spccially or temporally. If several devices can use the link simultaneously, it is spccially shared connection. If users must take turns, it is timeshared connection.

Physical Topology

The term physical topology refers to the way in which a network is laid out physically. Two or more devices connect to a link; two or more links form a topology. The topology of a network is the geometric representation of the relationship of all the links and linking devices (usually called nodes) to one another. Ther are four basic topologies possible: mesh, star, bus, and ring (see Fig. 1.4).



a. Point-to-point

b. Multipoint

Fig. 1.3 : Types of connections : point to point and multipoint

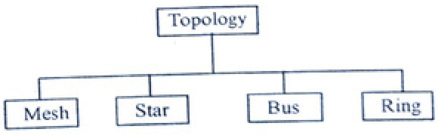


Fig. 1.4 : Categories of topology

Mesh Topology

Mesh In a mesh topology every device has a dedicated point-to-point link to every other device. The term dedicated means that the link carries traffic only between the two devices it connectes. To find the number of physical links in a fully connected mesh network with n nodes, we first consider that each node must be conected to every other node. Node 1 must be connected to n-1 nodes, node 2 must be connected to n-1 nodes, and finally node n must be connected to n-1 nodes. We need n(n - 1) physical links. However, if each physical link allows communication in both directions (duplex mode), we can divide the number of links by 2. In other words, we can say that in a mesh topology, e need.

$$n(n - 1)/2$$

duplex mode links.

To accomodate that many links, every device on the network must have n – 1 input/output (I/O) ports (see Figure 1.5) to be connected to the other n–1 stations.

A mesh offers several advantages over other network topologies. First, the use o dedicated links guarantees that each connection can carry its own data load, thus eliminating the traffic problems that can occur when links must be shared by multiple devices. Second, a mesh topology is robust. If one link becomes unusable, it does not incapacitate the entire system. Third, there is the advanage of privacy or security. When every message tavels along a dedicated line, only the intended recipient sees it. Physical boundaries prevent othe users from gaining access to messages. Finally, point-to-point links make fault identification and fault isolation easy. Traffic can be routed to avoid links with suspected problems. This facility enables the network manager to discover the precise location of the fault aids in finding its cause and solution.

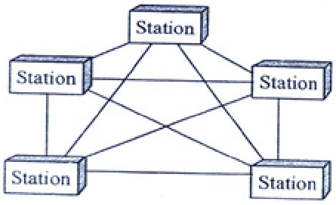


Fig. 1.5 : A fully connected mesh topology (five devices)

The main disadvantages of a mesh are related to the amount of cabling and the number of I/O ports required. First, because every device must be connected to every other device, installation and reconnection are difficult. Second, the sheer bulk of the wiring can be greater than the available space (in walls, ceilings, or floors) can accommodate. Finally the hardware required to connect each link (I/O ports and cable) can be prohibitively expensive. For these reasons a mesh topology is usually implemented in a limited fashion, for example, as a backbone connecting the main computers of a hybrid network that can include several other topologies.

One practical example of a mesh topology is the connection of telephone regional officers in which each regional office needs to be connected to every other regional office.

Star topology : In a star topology, each device has a dedicated point-to-point link only to a central controller, usually called a hub. The devices are not directly linked to one another. Unlike a mesh topology, a star topology does not allow direct traffic between devices. the controller acts as an exchange : If one device wants to send data to another, it sends the data to the controller, which then relays the data to the other connected device (see Figure 1.6).

A star topology is less expnesive than a mesh topology. In a star, each device needs only one link and one I/O port tc connect it to any number of others. This factor also makes it easy to install and reconfigure. Far less cabling needs to be housed, and additions, moves, and deletions involve only one connection: between that device and the hub.

Other advantages include robustness. If one link fails, only that link is affected. All other links remain active. This factor also lends itself to easy fault identification and fault isolation. As long as the hub is working, it can be used to monitor link problems and bypass defective links.

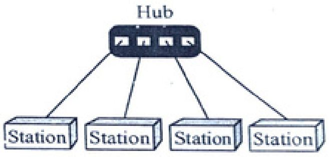


Fig. 1.6 : A star topology connecting four stations

One big disadvantage of a star topology isthe dependency of the whole topology one one single point, the hub. If the hub goes down, the whole system is dead.

Although a star requires far less cable than a mesh, each node must be linked to a central hub. For this reason, often more cabling is required in a star than in some other topoplogies (such as ring or bus).

The star topology is used in local-area network (LANs), as we wili see in Chapter 13. High speed LANs often use a star topology with a central hub.

Bus Topology : The preceding examples all describe point-to-point connections. A bus topology, on the other hand, is multipoint. One long cable acts as a backbone to link all the devices in a network (see Figure 1.7).

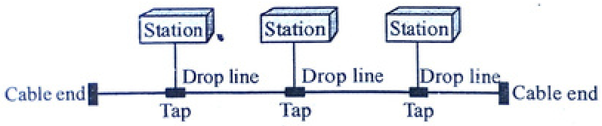


Fig. 1.7 : A bus topology connecting three stations

Nodes are connected to the bus cable by drop lines and taps. A drop line is a connection running between the device and the main cable. A tap is a connector that either splices into the main cable or punctures the sheating of a cable to create a contact with the metallic core. As a signal travels along the backbone, some of its energy is transformed into heat. Therefore, it becomes weaker and weaker as it travels farther and farther. For this reason there is a limit on the number of taps a bus can support and one the distance between those taps.

Advantages of a bus topology include ease of installation. Backbone cable can be laid along the most efficient path, then connected to the nodes by drop lines of various lengths. In this way, a bus uses less cabiing than mesh or star topologies. In a star, for example, four network devices in the same room require four lengths of cable reaching all the way to the hub. In a bus, this redundancy is eliminated. Only the backbone cable stretches through the entire facility. Each drop line has to reach only as far as the nearest point on the backbone.

Disadvantages include difficult reconnection and fault isolation. A bus is usually designed to be optimally efficient at installation. It can therefore be difficult to add new devices. Signal reflection at the taps can cause degradation in quality. This degradation can be controlled by limiting the number and spacing of devices connected to a given length of cable. Adding new devices may therefore require modification or replacement of the backbone.

In additicn, a fault or break in the bus cable stops all transmission, even between devices on the same side of the problem. The damaged area reflects signals back is the direction of origin, creating noise in both directions.

Bus topology was the one of the first topologies used in the design of early local area networks. Ethernet LANs can use a bus topology, but they are less popular now for reasons we will discuss in Chapter 13.

Ring Topology : In a ring topology, each device has a dedicated point-to-point connection with only the two devices on either side of it. A signal is passed along the ring in one direction, from device to device, ntil it reaches its destination. Each device in the ring incorporates a repeater. When a device receives a signal intended for another device, its repeater regenerates the bits and passes them along (see Figure 1.8).

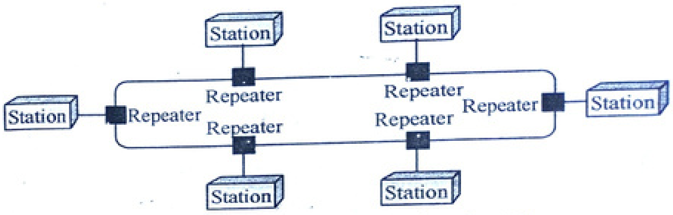


Fig. 1.8 : A ring topology connecting six stations

A ring is relatively easy to install and reconfigure. Each device is linked to only its immediate neighbors (eiter physically or logically). To add or delete a device requires changing only two connections. The only constraints are media and traffic considerations (maximum ring length and number of devices). In addition, fault isolation is simplified. Generally in a ring, a signal is circulating at all times. If one device does not receive a signal within a specified period, it can issue an alarm. The alarm alerts the network operator to the problem and its location.

However, unidirectional traffic can be a disadvantage. In a simple ring, a break in the ring (such as a disabled station) can disable the entire network. This weakness can be solved by using a dual ring or a switch capable of closing off the break.

Ring topology was prevalent when IBM introduced its local-area network Token Ring. Today, he need for higher speed LANs has made this topology less popular.

Hybrid Topology : A network can be hybrid. For example, we canhave a main star topology with each branch connecting several stations in a bus topology as shown in Figure 1.9.

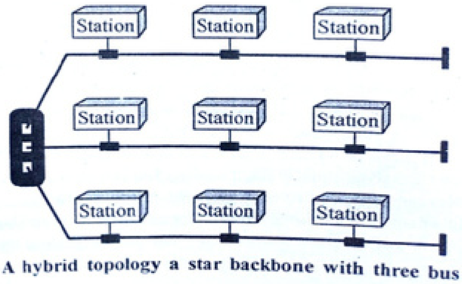


Fig. 1.9 : A hybrid topology a star backbone with three bus networks

Network Models

Computer networks are created by different entities. Standards are needed so that these heterogenous networks can communicate with one another. The two best known standards are the OSI model and the Internet model. In Chapter 2 we discuss these two models. The OSI (Open Systems Interconnection) model defines a seven-layer network; the Internet model defines a five-layer network. Thisbook is based on the Internet model with occasional references to the OSI model.

1.8 Data Transmission Modes

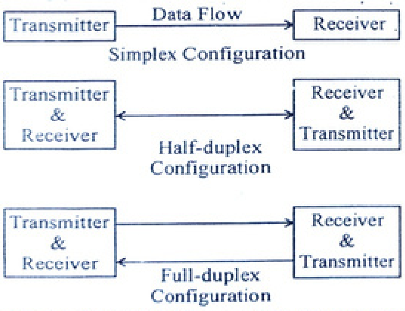
There are three modes of data transmission that correspond to the three types of circuits available (see fig.) These are :

(a) Simplex

(b) Half duplex

(c) Full-duplex.

(a) Simplex : Simplex communications imply a simple method of communicating which they are. In simplex communication mode, there is a one way communication transmission. Televisions transmission is a good example of simplex communications. The main transmitter sends out a signal (broadcast) but it does not expect a reply as the receiving units cannot issue a reply.



back to the transmitter. A data collection terminal one a factory floor (send only) or a line printer (receive only). Another example of simplex communication is a keyboard attached to a computer because the keyboard can only send data to the computer.

At first thought it might appear adequate for many types of application in which flow of information is unidirectional. However, in almost all data processing applications, communication in both directions is required. Even for a "one-way" flow of information from a terminal to a computer, the system will be designed to allow the computer to signal the terminal that data has been received without this capability, the remote user might enter data and never know that it was not received by te other terminal. Hence, simplex circuits are seldom used because a return path is generally needed to send acknowledgement control or error signals.

Half duplex : In half duplex mode, both units communicate over the same medium, but only one unit can send at a time. While one is in send mode, the other unit is in receive mode. It is like two polite people talking to each other one talks, the other listens, but neither one talks at the same time thus a half duplex line can alternately send and receive data. It requires two wires. This is the most common type of transmission for voice communications because only one person is supposed to speak at a time. It is also used to conncet a terminal with a computer. The terminal might transmit data and then the computer responds with an ancknowledgement. The transmission of data to and from a harddisk is also done in half duplex mode.

Full duplex : In a half-duplex system. Theline must be "turned around" each time the direction is reversed. 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 applications require simultaneous transmission in both directions (in such cases, a full duplex system is used that allows information to flow simultaneously in both direction on the transmission path. Use of a full duplex line improves efficiency as the line turn around time required in a half duplex arrangement is eliminated. It requires four wires.

Asynchronous And Synchronous Data Transmission

Asynchronous : Asynchronous refers to a series of events that take place which are not synchronized one after the other for example, the time interval between event A and B is not the same as B and C.

Asynchronous Communications : Asynchronous communication is often referred to as start up transmission because of the nature that is the sender can send a character at any time convenient and the receiver will accept it. Asynchronous communication lines remain in an idle state until the hardware on the line is ready to transmit. Since the line is idle, a series of bits has to be sent to the receiving node to notify it that there is data coming. When data is finished, the node has to be notified that the transmission is complete and to go back to an idle state, hence the stop bits are to be sent. This pattern continues for the duration of the time the link is operative. This is the characteristric of many terminals when on a terminal, the time spent between successive key strokes would vary. Thus in asynchronous transmission, data is transmitted character by character at irreglar intervals.

Synchronous devices usually do not use start and stop bit, so coordination between the two nodes i.e. The sender and the receiver is handled differently. In synchronous communication, there are two "channels" one for data and another for link synchronization. The channel for synchronization uses the integral clock in the hardware for link synchronization between the two nodes when one of the nodes is ready to transmit data, a unique combination o bits called a sync. character is sent to the receiver. Since the first character will probably get transhed a second one usually follows to ensure that synchronization is complete.

Synchronous mode of data transmission involves blocking a group of character in some what the same way records are blocked on magnetic tape. Each block is then framed by header and trailer information. The header consist of synchronizing information which is used by the receiving device to set its clock in synchronism with the sending end clock. The header also contains information to identify sender and receiver. Following the header is a block of characters that contains the actual message to be transmitted. The number of characters may be variable and may consist of hundreds of characters. The message characters in the block are terminated by a trailer. The trailer contain an end of message character followed by a check character to aid detection of any transmission error. Thus with synchronous transmission entire blocks of characters are framed and transmitted together.

Asyncronous transmission is well suited to many keyboard type terminals. The advantage of this method is that it does not require any local storage at the terminal or the computer as transmission takes place character by character. Hencė it is cheaper to implement. The main disadvantage of asynchronous transmission is that the transmission line is idle during the time intervals between transmitting character. If there are short, this is not bad because line cost would be low and idle time not expensive. Even through less efficient than synchronous transmission, it is also used with devices such as card reader and printer to reduce cost.

Efficiency of data transmission in synchronous and Asynchronous Modes

. Asynchronous data incorporates the use of extra framing bits to establish the start and ending (stop) of a data character word. A receiver responds to the data stream wen it detects a start bit. A data character is decoded and defined fte the stop bit is received and confirmed.

Asynchronous data are easier to detect and synchronize, but the efficiency of data transmission is reduced by the addition of framming bits as overhead (no message data) bit. A comparison of a single character using the two data type is as follows.

For this purpose, the significant bit (LSB) first. The number of framing bits used for asynchronous data varies depending on the stations in the communication link.

For example, suppose we use 1 start and 2 stop bits. This adds 3 addition bits tothe character word. Hence total 10 bits ar required to send the letter E using asynchronous data. However, in the case of synchronous transmissio, only 7 bits are required for transmission of the character E.

The efficiency to transmission is defined as the ratio of the number of message bits to the total number of transmitted bit :

$$\text{or efficiency} = \frac{\text{data bits}}{\text{total bits}} \times 100\%$$

As seen in the above exampl for the letter E. i.e. 1000101, the synchronous mode, all bits cary message so 100% efficiency is there.

However, in asynchronous mode, E is transmitted by using 7 bits as message and another three bits (one. start bit and two stop bits) totaling 10 bits so the efficiency is calculated as :

$$\text{Efficiency} = \frac{\text{data bits i.e. } 7}{\text{total bits i.e. } 10} \times 100\% = 70\%$$

1.9 The Internet

The Internet has revolutionized many aspects of our daily lives. It has affected the way we do business as well as the way we spend our leisure time. Count the ways you've used the Internet recently. Perhaps you've sent electronic mail (e-mail) to a business associate, paid a utility bill, read a newspaper from a distant city, or looked up a local movie schedule-all by using the Internet. Or may be you researched a medical topic, booked a hotel reservation, chatted with a fellow Trekkie, or comparison-shopped for a car. The Internet is a communication system that has brought a wealth of information to our fingerips and organized it for our use.

The Internet is a structured, organized system. We begin with a brief history of the Internet. We follow with a description of the Internet today.

1.10 A Brief History

A network is a group of connected communicating devices such as computers and printers. An internet (note the lowercase letter i) is two or more networks that can communicate with each other. The most notable internet is called the Internet (uppercase letter I), a collaboration of more than hundreds of thousands of interconnected networks. Private individuals as well as various organiztions such as government agencies, schools, research facilities, corporations, and libraties in more than 100 countries use the Internet. Millions of people are users. Yet this extraordinary communication system only came into being in 1969.

In the mid 1960s, mainframe computers in research organizations were stand alone devices. Computers from different manufactures were unable to communicate with one another. The Advanced Research Projects Agency (ARPA) in the Department of Defense (DoD) was interested in finding a way to connect computers so that the researchers they funded coul share their findings,thereby reducing costs and eliminating duplication of effort.

In 1967, at an Association for computing Machinery (ACM) meeting, ARPA presented its ideas for ARPANET, a small network of connected computers. The idea was that each host computer (not necessarily from the same manufacturer) would be attached to a specialized computer, called an interface message processor (IMP). The IMPs in turn, would be connected to on another. Each IMP had to be able to communicate with other IMPs as well as with its own attached host.

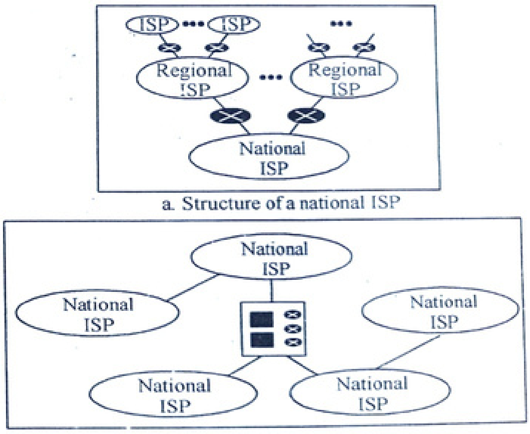
By 1969, ARPANET was a reality. Four nodes, at the University of Californa at Los Angeles (UCLA), the university of California at Santa Barbara (UCSB), Stanford Research Institute (SRI), and the University of Utah, were connected via the IMPs to form a network. Software called the Network Control Protocol (NCP) provided communication between the hosts.

In 1972, Vint Cerf and Bob Kahn, both of whom were part o the core ARPANET group, collaborated on what they called the Internetting project. Cerf and Kahn's land mark 1973 paper outlined the protocols to achieve end to end delivery of packets. This paper on transmission Control Protocol (TCP) included concepts such as encapsulation, the datagram, and the functions of a gateway.

Shortly thereafter, authorities made a decision to split TCP into two protocols : Transmission Control Protocol (TCP) and Internetworking Protocol (IP). IP would handle datagram routing while TCP would be responsible for higher level functions such as segmentation, reassembly, and error detection. The internetworking protocol became known as TCP/IP.

1.11 The Internet Today

The Internet has come a long way since the 1960s. The Internet today is not a simple hierarchical structure. It is made up of many wide and local area networks joined by connecting devices and switching stations. It is difficult to give an accurate representation of the Internet because it is continually changing new networks are being added, existing networks are adding address, and networks of defunct companies are being removed. Today most end users who want Internet connection use the services of Internet service providers (ISPs). There are international service providers, national service providers, regional service providers, and local service providers. The Internet today is run by private companies, not the government. Figure 1.13 shows a conceptual (not geographic) view of the Internet.



a. Structure of a national ISP

b. Interconnection of national ISPs

Fig. 1.13 : Hierarchical Organization of the Internet

International Internet Service Providers

At the top of the hierarchy are the international service providers that connect national together.

National Internet Service Providers

The national Internet service providers are backbone network created and maintained by specialized companies. There are many national ISPs operating in

Non America; some of the most well known are Sprintlink, PSI Net, UUNet Technology AGIS, and internet MCI. To provide connectivity between the end users, these back bone networks are connected by complex switching stations (normally rn by a tird party) called network access points (NAPs). Some national ISP networks are also connected to one another by private switching stations called peering points. These normally operate at a high data rate (up to 600 Mbps).

Regional Internet Service Providers

Regional internet service providers or regional ISPs are smaller ISPs that are connected to one or more national ISPs. They are at the third level of the hierarcy with a smaller data rate.

Local Internet Service Providers

Local Internet Service providers provide direct service to the end users. The local ISPs can be connected to regional ISPs or directly to national ISPs. Most and users are connected to the local ISPs. Note that in this sense, a local ISP can be a company that just provides Internet services, a corporation with a network that supplies services to its own employees or a nonprofit organization, such as a college or a university, that runs its own network. Each of these loal ISPs can be connected to a regional or national service provider.

1.12 Protocols and Standards

In this section, we define two widely used terms; protocols and standard. First, we define protocol, which is synonymous with rule. Then we discuss standards, which are agreed upon rules.

Protocols

In computer networks, communication occurs between entities in different systems. An entity is anything capable of sending or receiving information. However, two entities can not simply send bit streams to each other and expect to be undestood. For communication to occur, the entities must agree on a protocol. A protocol is a set of rules that govern data communications. A protocol defines whhat is communicated, how it is communicated, and when it is communicated. The key elements of a protocol are syntax, semantics, and timing.

Syntax : The term syntax refers to the structure or format of the data, meaning the order in which they are presented. For example, a simple protocol might expect the first 8 bits of data to be the address of the sender, the second 8 bits to be the address of the receiver, and the rest of the stream ot be the message itself.

Semantics : The word semantics refers to the meaning of each section of bits. How is a particular pattern to be interpreted, and what action is to be takne based on that interpretation ? For example, does an address identify the route to be taken or the final destination of the message ?

Timing : The term timing refers to two characteristics : wen data should be sent and how fast they can be sent. For example, if a sender produces data at 100 Mbps but the receiver can process data at only 1 Mbps, the transmission will overload the receiver and some data will be lost.

Standards

Standards are essential in creating and maintaining an open and competitive market for equipment manufacturers and in guaranteeing national and international interoperability of data and telecommunications technology and processes. Standards provide guidelines to manufactoures, vendors, government agencies, and other service providers to ensure the kind of interconnectivity necessary in today's marketplace and in international communications. Data communication standards fall into two categories : de facto (meaning "by fact" or "by convention") and de jure (meaning "by law" or "by regulation").

De facto : Standards that have not been approved by an organized body but have been adopted as standards through widespread use are de facto standards. De fecto standards are often established originally by manufacturers who seek to define the functionality of a new product or technology.

De jure : Those standars that have been legislated by an officially recognized body are de jure standards.

Standards Organizations

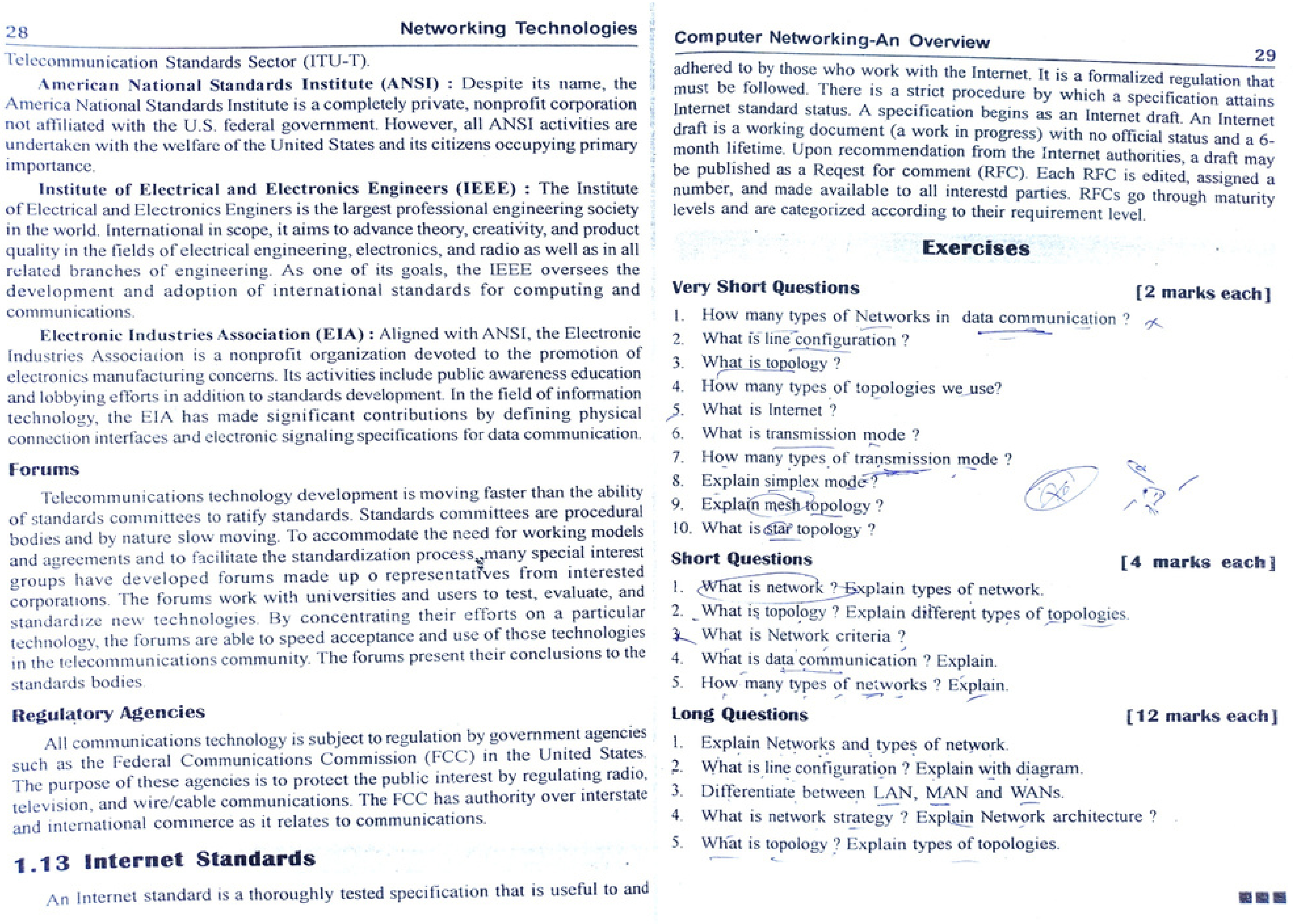
Standards are developed through the cooperation of standards creation committees, forums, and government regulatory agencies.

Standards Creation Committees

While many orgnizations are dedicated to the establishment of standards, data telecommunications in North America rely primarily on tose published by the following :

International Organization for Standardization (ISO) : The ISO is a multinational body whose membership is drawn mainly from the standards creation committees of various goernments throughout the world. The ISO is active in developing cooperation in the realms of scientific, technological, and economic activity.

International Telecommunication Union-Telecommunication Standards Sector (ITU-T) : By the early 1970s, a number of countries were defining national standards for telecommunications, but there was still little international compatibility. The United Nations responded by forming, as part of its International Telecommunication Union (ITU), a committee, the Consultative Committee for International Telegraphy and Telephony (CCITT). This committee was devoted to the research and establishment of standards for telecommunications in general and for phone and data systems in particular. On March 1, 1993, the name of this committee was changed to the International Telecommunication Union



Telecommunication Standards Sector (ITU-T).

American National Standards Institute (ANSI) : Despite its name, the America National Standards Institute is a completely private, nonprofit corporation not affiliated with the U.S. federal government. However, all ANSI activities are undertaken with the welfare of the United States and its citizens occupying primary importance.

Institute of Electrical and Electronics Engineers (IEEE) : The Institute of Electrical and Electronics Enginers is the largest professional engineering society in the world. International in scope, it aims to advance theory, creativity, and product quality in the fields of electrical engineering, electronics, and radio as well as in all related branches of engineering. As one of its goals, the IEEE oversees the development and adoption of international standards for computing and communications.

Electronic Industries Association (EIA) : Aligned with ANSI, the Electronic Industries Association is a nonprofit organization devoted to the promotion of electronics manufacturing concerns. Its activities include public awareness education and lobbying efforts in addition to standards development. In the field of information technology, the EIA has made significant contributions by defining physical connection interfaces and electronic signaling specifications for data communication.

Forums

Telecommunications technology development is moving faster than the ability of standards committees to ratify standards. Standards committees are procedural bodies and by nature slow moving. To accommodate the need for working models and agreements and to facilitate the standardization process, many special interest groups have developed forums made up o representatives from interested corporations. The forums work with universities and users to test, evaluate, and standardize new technologies. By concentrating their efforts on a particular technology, the forums are able to speed acceptance and use of those technologies in the telecommunications community. The forums present their conclusions to the standards bodies.

Regulatory Agencies

All communications technology is subject to regulation by government agencies such as the Federal Communications Commission (FCC) in the United States. The purpose of these agencies is to protect the public interest by regulating radio, television, and wire/cable communications. The FCC has authority over interstate and international commerce as it relates to communications.

1.13 Internet Standards

An Internet standard is a thoroughly tested specification that is useful to and

adhered to by those who work with the Internet. It is a formalized regulation that must be followed. There is a strict procedure by which a specification attains Internet standard status. A specification begins as an Internet draft. An Internet draft is a working document (a work in progress) with no official status and a 6-month lifetime. Upon recommendation from the Internet authorities, a draft may be published as a Reqest for comment (RFC). Each RFC is edited, assigned a number, and made available to all interestd parties. RFCs go through maturity levels and are categorized according to their requirement level.

Exercises

Very Short Questions [2 marks each]

1. How many types of Networks in data communication ?
2. What is line configuration ?
3. What is topology ?
4. How many types of topologies we use?
5. What is Internet ?
6. What is transmission mode ?
7. How many types of transmission mode ?
8. Explain simplex mode ?
9. Explain mesh topology ?
10. What is star topology ?

Short Questions [4 marks each]

1. What is network ? Explain types of network.
2. What is topology ? Explain different types of topologies.
3. What is Network criteria ?
4. What is data communication ? Explain.
5. How many types of networks ? Explain.

Long Questions [12 marks each]

1. Explain Networks and types of network.
2. What is line configuration ? Explain with diagram.
3. Differentiate between LAN, MAN and WANs.
4. What is network strategy ? Explain Network architecture ?
5. What is topology ? Explain types of topologies.