NounElearn
www.nounelearn.com
@NounElearn 07018870798

CIT303 - PRINCIPLES OF COMMUNICATION TECH. SUMMARY

Q. Explain data communication and outline and explain their features.

Data Communications

Data communications is the exchange of data between two devices via some form of transmission medium such as a wire cable. For data communications to occur, the communicating devices must be part of a communication 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, timeliness, and jitter.

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 are unusable.

3. Timeliness: The system must deliver data in a timely manner. Data delivered late are useless. In the case of video and audio, timely delivery 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.

4. Jitter: Jitter 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. If some of the packets arrive with 30-ms delay and others with 40-ms delay, an uneven quality in the video is the result.

Q. Describe with diagram the components of data communication

Components Involved in Data Communication

A data communications system has five components (see Figure 1.1).

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: The transmission medium is the path by which a message travels from sender to receiver. Some examples of transmission media include twisted-pair wire, coaxial cable, fiberoptic cable, and radio waves. 5. Protocol. A protocol is a set of rules that govern data communications. It sents an agreement between the communicating devices. Without a protocol, devices may be connected but not communicating, just as a person speaking Fr cannot be understood by a person who speaks only Japanese.

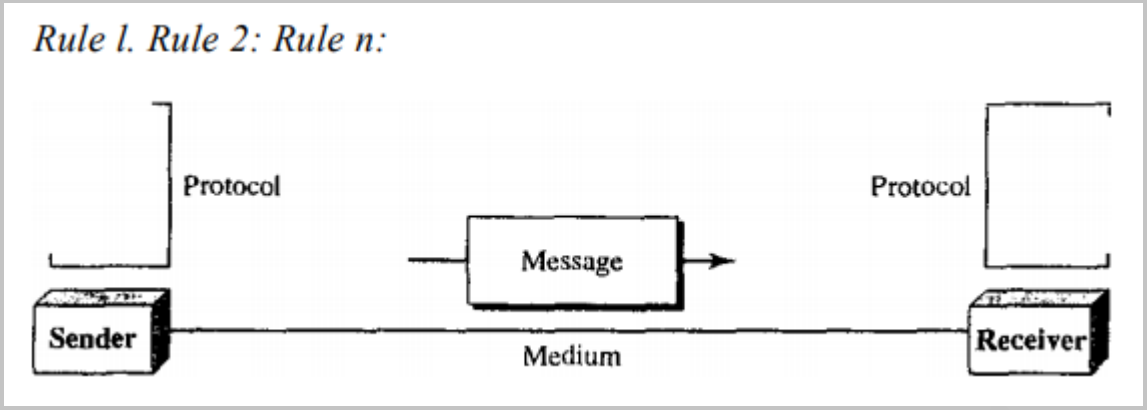


Figure 1.1 Five components of data communication

Q. Give a list of possible data representation in data communication.

Data Representation

1. Text

2. Numbers

3. Images

4. Audio

5. Video

Q. Briefly describe each of the data representation identified above and the form of their preparation for transmission.

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

1. Text

In data communications, text is represented as a bit pattern, a sequence of bits (Is). Different sets of bit patterns have been designed to represent text symbols. Each is called a code, and the process of representing symbols is called coding. Today prevalent coding system is called Unicode, which uses 32 bits to represent a symbol character used in any language in the world. The American Standard Code for Information Interchange (ASCII), developed some decades ago in the United States, constitutes the first 127 characters in Unicode and is also referred to as Basic Latin.

2. Numbers

Numbers are also represented by bit patterns. However, a code such as ASCII is not t to represent numbers; the number is directly converted to a binary number to simple mathematical operations.

3. Images

Images are also represented by bit patterns. In its simplest form, an image is compound of a matrix of pixels (picture elements), where each pixel is a small dot. The size of pixel depends on the resolution. For example, an image can be divided into 1000 pi: or 10,000 pixels. In the second case, there is a better representation of the image (be resolution), but more memory is needed to store the image. After an image is divided into pixels, each pixel is assigned a bit pattern. The value of the pattern

depends 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.

There are several methods to represent color images. One method is called RGB so called because each color is made of a combination of three primary colors: red green, and blue. The intensity of each color is measured, and a bit pattern is assignee it. Another method is called YCM, in which a color is made of a combination of the other primary colors: yellow, cyan, and magenta.

4. Audio

Audio refers to the recording or broadcasting of sound or music. Audio is by nature different from text, numbers, 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.

5. Video

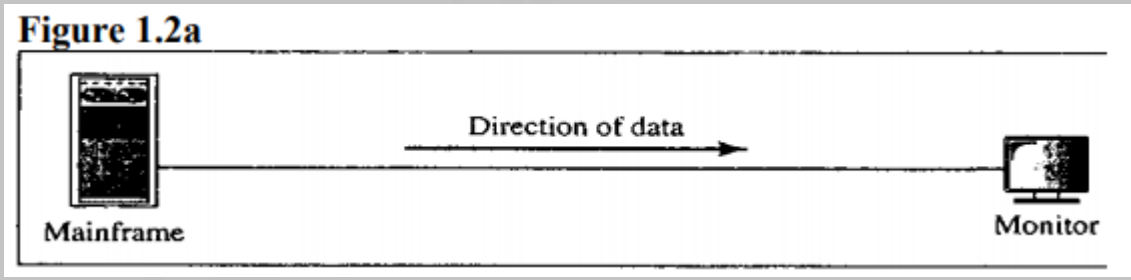
Video refers to the recording or broadcasting of a picture or movie. Video can either be produced as a continuous entity (e.g., by a TV camera), or it can be a combination of images, each a discrete entity, arranged to convey the idea of motion.

Q. Explain data flow.

Data Flow

1. Simplex

In simplex mode, the communication is unidirectional, as on a one-way street. Only one of the two devices on a link can transmit; the other can only receive (see Figure 1.2a). Keyboards and traditional monitors are examples of simplex devices. The keyboard can only introduce input; the monitor can only accept output. The simplex mode can use the entire capacity of the channel to send data in one direction.



Communication between two devices can be simplex, half-duplex, or full -duplex as shown in Figure 1.2. (a, b & c)

2. Half-Duplex

In half-duplex mode, each station can both transmit and receive, but not at the same time. When one device is sending, the other can only receive, and vice versa. The half-duplex mode is like a one-lane road with traffic allowed in both directions. When cars are traveling in one direction, cars going the other way must wait. half-duplex transmission, the entire capacity of a channel is taken over by whichever the two devices is transmitting at the time. Walkie-talkies and CB (citizens band) are both half-duplex systems. The half-duplex mode is used in cases where there is no need for communicate, in both directions at the same time; the entire capacity of the channel can be utilized each direction.

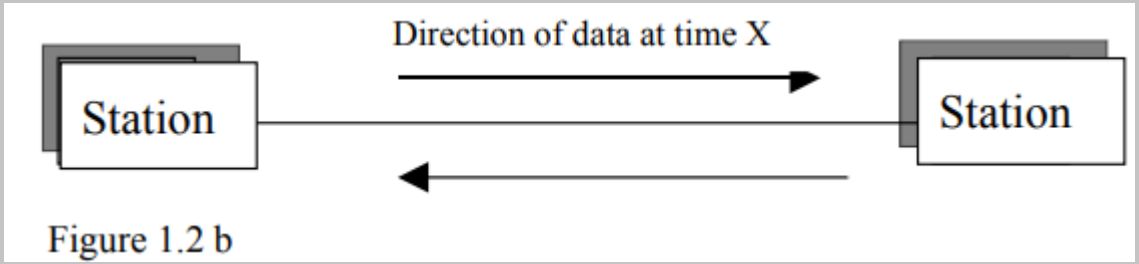


Figure 1.2 b

3. Full-Duplex

In full-duplex mode (also called duplex), both stations can transmit and receive simultaneously (see Figure 1.2c). The full-duplex mode is like a two-way street with traffic flowing in both directions at the same time. In full-duplex mode, signals going in one direction share capacity of the link with signals going in the other direction. This sharing can occur in two ways: Either the link must contain two physically separate transmission paths, for sending and the other for receiving; or the capacity of the channel is division between signals traveling in both directions.

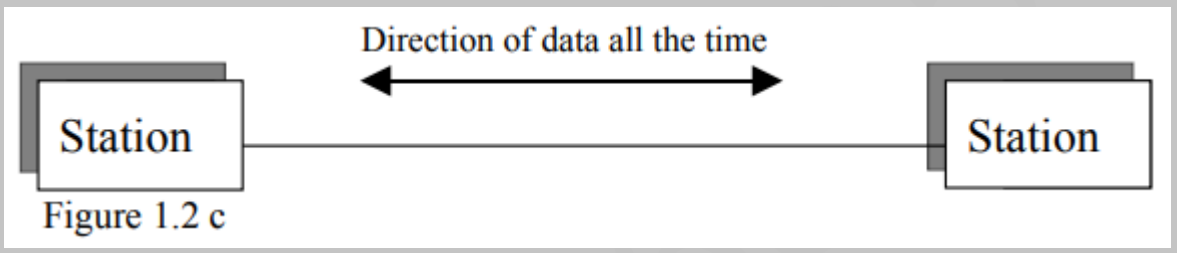


Figure 1.2 c

One common example of full-duplex communication is the telephone network. When two people are communicating by a telephone line, both can talk and listen at same time. The full-duplex mode is used when communication in both directions is requires all the time. The capacity of the channel, however, must be divided between the t directions.

Q. What is a computer network?

Computer Network

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

Q. Briefly explain distributed processing

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 process, separate computers (usually a personal computer or workstation) handle subset.

Q. Outline and explain three Network criteria

Network Criteria

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

1. Performance

Performance can be measured in many ways, including transit time and response time. Transmit 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 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, zinc) the efficiency of the software.

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

2. 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's robustness in a catastrophe.

3. 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 losses.

Q. Discuss the two possible types of connections.

Types of Network Connections

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.

1. 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.

2. Multipoint

A multipoint (also called multidrop) connection is one in which more than two specific devices share a single link (see Figure 1.36). In a multipoint environment, the capacity of the channel is shared, either spatially or temporally. It' sever al devices can use the link simultaneously; it is a spatially shared connection. If users must take turns, it is a timeshared connection.

Q. Explain what is meant by the physical topology of a network

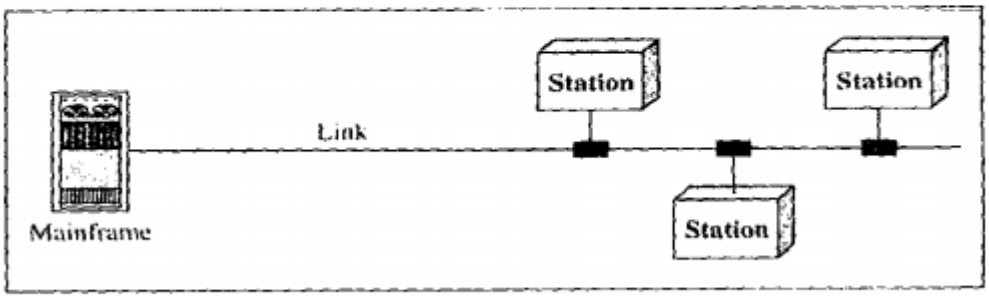
Network Physical Topology

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 line linking devices (usually called nodes) to one another. There are four basic tope possible: mesh, star, bus, and ring (see Figure 1.4).

Figure 1.3 Types of connections: point-to-point and multipoint



a. point-to-point



b. Multipoint

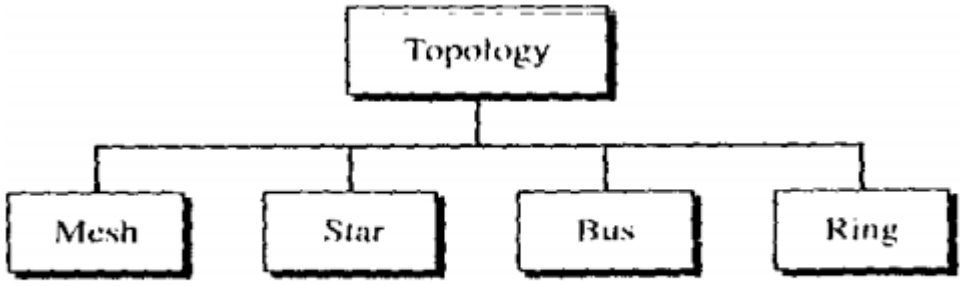


Figure 1.4 Categories of topology

Q. What is a protocol and list and explain its key elements?

Protocols

In computer networks, communication occur between entities in different system entity is anything capable of sending or receiving information. However, two entities not simply send bit streams to each other and expect to be understood. For communicate to occur, the entities must agree on a protocol. A protocol is a set of rules that govern communications. A protocol defines what is communicated, how it is communicate when it is communicated.

The key elements of a protocol are syntax, semantics, and timing.

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

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

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

Q. Why are standards necessary in data communications?

Importance of Standards

Standards are essential in creating and maintaining open and competitive marl equipment manufacturers and in guaranteeing national and international interposer of data and telecommunications technology and processes. Standards provide guide to manufacturers, vendors, government agencies, and outer 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 jute (meaning "by law" or "by regulation").

i. 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 facto standards are often established originally by manufacturers who seek to define the functionality of a new product or technology.

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

Standards Organization

i. International Organization for Standardization (ISO)

The ISO is a multinational body whose membership is drawn mainly from the standards creation committees of various governments throughout the world. The ISO is active in developing cooperation in the realms of scientific, technological, and economic activity.

ii. 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 l, 1993, the name of this committee was changed to the International Telecommunication Union Telecommunication Standards Sector (ITU-T).

iii. American National Standards Institute (ANSI)

Despite its name, the American 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.

iv. Institute of Electrical and Electronics Engineers (IEEE)

The Institute of Electrical and Electronics Engineers 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.

v. 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 inform; technology, the EIA has made significant contributions by defining physical connotation interfaces and electronic signaling specifications for data communication.

Q. Discuss internet standards

An Internet standard is thoroughly tested specifications that is useful to and adhere to by those who work with the Internet. It is a formalized regulation that must be lower. There is a strict procedure by which a specification attains Internet stand 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 Request Comment (RFC). Each RFC is edited, assigned a number, and made available to interested parties. RFCs go through maturity levels and are categorized according their requirement level.

Q. What is OSI?

OSI: Physical Layer

The Open System Interconnection Reference Model (OSI Reference Model or OSI Model) is an abstract description for layered communications and computer network protocol design. It was developed as part of the Open Systems Interconnection (OSI) initiative. In its most basic form, it divides network architecture into seven layers which, from top to bottom, are the Application, Presentation, Session, Transport, Network, Data-Link, and Physical Layers. It is therefore often referred to as the OSI Seven Layer Model.

A layer is a collection of conceptually similar functions that provide services to the layer above it and receives service from the layer below it. On each layer an instance provides services to the instances at the layer above and requests service from the layer below. For example, a layer that provides error-free communications across a network provides the path needed by applications above it, while it calls the next lower layer to send and receive packets that make up the contents of the path. Conceptually two instances at one layer are connected by a horizontal protocol connection on that layer.

Q. Explain the Physical layer

Physical Layer

The Physical Layer is the first and lowest layer in the seven-layer OSI model of computer networking. The Physical Layer consists of the basic hardware transmission technologies of a network. It is a fundamental layer underlying the logical data structures of the higher level functions in a network. Due to the plethora of available hardware technologies with widely varying characteristics, this is perhaps the most complex layer in the OSI architecture. The implementation of this layer is often termed PHY.

The Physical Layer defines the means of transmitting raw bits rather than logical data packets over a physical link connecting network nodes. The bit stream may be grouped into code words or symbols and converted to a physical signal that is transmitted over a hardware transmission medium. The Physical Layer provides an electrical, mechanical, and procedural interface to the transmission medium. The shapes and properties of the electrical connectors, the frequencies to broadcast on, the modulation scheme to use and similar low-level parameters, are specified here.

Within the semantics of the OSI network architecture, the Physical Layer translates logical communications requests from the Data Link Layer into hardware-specific operations to effect transmission or reception of electronic signals.

Q. Explain the Physical signaling sub-layer

Physical Signaling Sub Layer

In a local area network (LAN) or a metropolitan area network (MAN) using open systems interconnection (OSI) architecture, the physical signaling sublayer is the portion of the Physical Layer that:

• interfaces with the medium access control sublayer (MAC) which is a part of the Data Link Layer

• performs character encoding, transmission, reception and decoding.

• performs mandatory isolation functions.

Q. What are the major functions and services performed by the Physical Layer?

List of Physical Layer Services

The major functions and services performed by the Physical Layer are:

i. Bit-by-bit or symbol-by-symbol delivery

ii. Providing a standardized interface to physical transmission media, including

- Mechanical specification of electrical connectors and cables, for example maximum cable length
- Electrical specification of transmission line signal level and impedance
- Radio interface, including electromagnetic spectrum frequency allocation and specification of signal strength, analog bandwidth, etc.
- Specifications for IR over optical fiber or a wireless IR communication link

iii. Modulation

iv. Line coding

v. Bit synchronization in synchronous serial communication

vi. Start-stop signaling and flow control in asynchronous serial communication

vii. Circuit switching

viii. Multiplexing

ix. Equalization filtering, training sequences, pulse shaping and other signal processing of physical signals

x. Forward error correction for example bitwise convolution coding

Examples of Physical Layer

1. Telephone network modems- V.92
2. IRDA Physical Layer
3. USB Physical Layer
4. Ethernet physical layer
5. Varieties of 802.11 Wi-Fi Physical Layers
6. DSL
7. ISDN
8. T1 and other T-carrier links, and E1 and other E-carrier links
9. SONET/SDH
10. Firewire

Examples of Hardware Equipment (Network Node)

1. Network adapter
2. Repeater
3. Network hub
4. Modem

5. Fiber Media Converter

Relation to TCP/IP Model

The TCP/IP model is a high-level networking description used for the Internet and similar networks. It does not define an equivalent layer that deals exclusively with hardware-level specifications, as this model does not concern itself directly with physical interfaces. It specifies a functioning host operating system with a facility to transmit packets onto the local network via a local area network encapsulation method (e.g., RFC 1042). and simply absorbs all hardware specific components of the operating system and interface firmware into the Link Layer without detailed specifications. The TCP/IP model is not a top/down comprehensive design reference for general networks and networking hardware, but an architectural description of the suite of methods and requirements used in the Internet Protocol Suite to achieve internetworking between disparate local area networks.

Q. What is Data link layer?

Data Link Layer

The Data Link Layer is the protocol layer which transfers data between adjacent network nodes in a wide area network or between nodes on the same local area network segment. The Data Link Layer provides the functional and procedural means to transfer data between network entities and might provide the means to detect and possibly correct errors that may occur in the Physical Layer. Examples of data link protocols are Ethernet for local area networks (multi-node), the Point-to-Point Protocol (PPP), HDLC and ADCCP for point-to-point (dual-node) connections.

The Data Link Layer is concerned with local delivery of frames between devices on the same LAN. Data Link frames, as these protocol data units are called, do not cross the boundaries of a local network. Inter-network routing and global addressing are higher layer functions, allowing Data Link protocols to focus on local delivery, addressing, and media arbitration. In this way, the Data Link layer is analogous to a neighborhood traffic cop; it endeavors to arbitrate between parties contending for access to a medium. When devices attempt to use a medium simultaneously, frame collisions occur. Data Link protocols specify how devices detect and recover from such collisions, but it does not prevent them from happening.

Delivery of frames by layer 2 devices is effected through the use of unambiguous hardware addresses. A frame's header contains source and destination addresses that indicate which device originated the frame and which device is expected to receive and process it. In contrast to the hierarchical and routable addresses of the network layer, layer 2 addresses are flat, meaning that no part of the address can be used to identify the logical or physical group to which the address belongs.

The data link thus provides data transfer across the physical link. That transfer can be reliable or unreliable; many data link protocols do not have acknowledgments of successful frame reception and acceptance, and some data link protocols might not even have any form of checksum to check for transmission errors. In those cases, higher-level protocols must provide flow control, error checking, and acknowledgments and retransmission. Within the semantics of the OSI network architecture, the Data Link Layer protocols respond to service requests from the Network Layer and they perform their function by issuing service requests to the Physical Layer.

Sub-layers of the Data Link Layer

i. Logical Link Control sublayer

The uppermost sublayer is Logical Link Control (LLC). This sublayer multiplexes protocols running atop the Data Link Layer, and optionally provides flow control, acknowledgment, and error notification. The LLC provides addressing and control of the data link. It specifies which mechanisms are to be used for addressing stations over the transmission medium and for controlling the data exchanged between the originator and recipient machines.

ii. Media Access Control sublayer

The sublayer below it is Media Access Control (MAC). Sometimes this refers to the sublayer that determines who is allowed to access the media at any one time (usually CSMA/CD). Other times it refers to a frame structure with MAC addresses inside.

There are generally two forms of media access control: **distributed** and **centralized**. Both of these may be compared to communication between people. In a network made up of people speaking, i.e. a conversation, we look for clues from our fellow talkers to see if any of them appear to be about to speak. If two people speak at the same time, they will back off and begin a long and elaborate game of saying "no, you first".

The Media Access Control sublayer also determines where one frame of data ends and the next one starts. There are four means of doing that: time based, character counting, byte stuffing and bit stuffing.

• The time based approach simply puts a specified amount of time between frames. The major drawback of this is that new gaps can be introduced or old gaps can be lost due to external influences.

• Character counting simply notes the count of remaining characters in the frame's header. This method, however, is easily disturbed if this field gets faulty in some way, thus making it hard to keep up synchronization.

• Byte stuffing precedes the frame with a special byte sequence such as DLE STX and succeeds it with DLE ETX. Appearances of DLE (byte value 0x10) has to be escaped with another DLE. The start and stop marks are detected at the receiver and removed as well as the inserted DLE characters.

• Similarly, bit stuffing replaces these start and end marks with flag consisting of a special bit pattern (e.g. a 0, six 1 bits and a 0). Occurrences of this bit pattern in the data to be transmitted is avoided by inserting a bit. To use the example where the flag is 01111110, a 0 is inserted after 5 consecutive 1's in the data stream. The flags and the inserted 0's are removed at the receiving end. This makes for arbitrary long frames and easy synchronization for the recipient. Note that this stuffed bit is added even if the following data bit is 0, which could not be mistaken for a sync sequence, so that the receiver can unambiguously distinguish stuffed bits from normal bits.

iii. Interfaces

The Data Link Layer is often implemented in software as a "network card driver". The operating system will have a defined software interface between the data link and the network transport stack above. This interface is not a layer itself, but rather a definition for interfacing between layers.

List of Data Link Layer Services

i. Encapsulation of network layer data packets into frames

ii. Frame synchronization

iii. Logical link control (LLC) sublayer

- Error control (automatic repeat request,ARQ)
- Flow control, in addition to one provided on the Transport layer.

iv. Media access control (MAC) sublayer:

- Multiple access protocols for channel-access control, for example CSMA/CD protocols for collision detection and retransmission in Ethernet bus networks and hub networks, or the CSMA/CA protocol for collision avoidance in wireless networks.

- Physical addressing (MAC addressing) o LAN switching (packet switching) including MAC filtering and spanning tree protocol
- Data packet queuing or scheduling o Store-and-forward switching or cut-through switching
- Quality of Service (QoS) control o Virtual LANs (VLAN)

Q. List 7 protocols of the data link layer

Protocol Examples

1. ARCnet
2. ATM
3. Cisco Discovery Protocol (CDP)
4. Controller Area Network (CAN)
5. Econet
6. Ethernet
7. Ethernet Automatic Protection Switching (EAPS)
8. Fiber Distributed Data Interface (FDDI)
9. Frame Relay
10. High-Level Data Link Control (HDLC)

Q. Discuss the data link layer relation to TCP/IP model

Relation to TCP/IP Model

In the frame work of the TCP/IP (Internet Protocol Suite) model, OSI's Data Link Layer, in addition to other components, is contained in TCP/IP's lowest layer, the Link Layer. The Internet Protocol's Link Layer only concerns itself with hardware issues to the point of obtaining hardware addresses for locating hosts on a physical network link and transmitting data frames onto the link. Thus, the Link Layer is broader in scope and encompasses all methods that affect the local link, which is the group of connections that are limited in scope to other nodes on the local access network.

The TCP/IP model is not a top/down comprehensive design reference for networks. It was formulated for the purpose of illustrating the logical groups and scopes of functions needed in the design of the suite of internetworking protocols of TCP/IP, as needed for the operation of the Internet. In general, direct or strict comparisons of the OSI and TCP/IP models should be avoided, because the layering in TCP/IP is not a principal design criterion and in general considered to be "harmful" (RFC 3439). In particular, TCP/IP does not dictate a strict hierarchical sequence of encapsulation requirements, as is attributed to OSI protocol.

Q. Define the Network layer

Network Layer

The Network Layer provides the functional and procedural means of transferring variable length data sequences from a source to a destination host via one or more networks while maintaining the quality of service and error control functions. The Network Layer is Layer 3 of the seven-layer OSI model of computer networking. The Network Layer is responsible for end-to-end (source to destination) packet delivery including routing through intermediate hosts, whereas the Data Link Layer is responsible for node-to-node (hop-to-hop) frame delivery on the same link.

Q. Discuss the functions of the network layer

Functions of the Network Layer

i. Connection model

Connection-oriented and connectionless communication. For example, snail mail is connectionless, in that a letter can travel from a sender to a recipient without the recipient having to do anything. On the other hand, the telephone system is connection-oriented, because the other party is required to pick up the phone before communication can be established. The OSI Network Layer protocol can be either connection-oriented, or connectionless. In contrast, the TCP/IP Internet Layer supports only the connectionless Internet Protocol (IP); but connection oriented protocols exist higher at other layers of that model.

ii. Host addressing

Every host in the network needs to have a unique address which determines where it is. This address will normally be assigned from a hierarchical system, so you can be "Fred Murphy" to people in your house, "Fred Murphy, Main Street 1" to Dubliners, or "Fred Murphy, Main Street 1, Dublin" to people in Ireland, or "Fred Murphy, Main Street 1, Dublin, Ireland" to people anywhere in the world. On the Internet, addresses are known as Internet Protocol (IP) addresses.

iii. Message forwarding

Since many networks are partitioned into sub networks and connect to other networks for wide-area communications, networks use specialized hosts, called gateways or routers to forward packets between networks. This is also of interest to mobile applications, where a user may move from one location to another, and it must be arranged that his messages follow him. Version 4 of the Internet Protocol (IPv4) was not designed with this feature in mind, although mobility extensions exist. IPv6 has a better designed solution.

Q. Write a brief note on the relation of the Network layer to TCP/IP model

Relation of the Network layer with TCP/IP

The TCP/IP model describes the protocol suite of the Internet. This model has a layer called the Internet Layer, located above the Link Layer. In many text books and other secondary references the Internet Layer is often equated with OSI's Network Layer. However, this is misleading as the allowed characteristics of protocols (e.g., whether they are connection-oriented or connection-less) placed into these layer are different in the two models. The Internet Layer of TCP/IP is in fact only a subset of functionality of the Network Layer. It only describes one type of network architecture, the Internet. In general, direct or strict comparisons between these models should be avoided, since the layering in TCP/IP is not a principal design criterion and in general is considered to be "harmful".

Q. What is the Transport Layer?

Transport Layer

The Transport Layer provides transparent transfer of data between end users, providing reliable data transfer services to the upper layers. The Transport Layer controls the reliability of a given link through flow control, segmentation/desegmentation, and error control. Some protocols are state and connection oriented. This means that the Transport Layer can keep track of the segments and retransmit those that fail.

Although not developed under the OSI Reference Model and not strictly conforming to the OSI definition of the Transport Layer, typical examples of Layer 4 are the Transmission Control Protocol (TCP) and User Datagram Protocol (UDP).

Of the actual OSI protocols, there are five classes of connection-mode transport protocols ranging from class 0 (which is also known as TP0 and provides the least error recovery) to class 4 (TP4, designed for less reliable networks, similar to the Internet). Class 0 contains no error recovery, and was designed for use on network layers that provide errorfree connections. Class 4 is closest to TCP, although TCP contains functions, such as the graceful close, which OSI assigns to the Session Layer.

Also, all OSI TP connection-mode protocol classes provide expedited data and preservation of record boundaries, both of which TCP is incapable. Detailed characteristics of TP0-4 classes are shown in the following table:

Feature Name	TP0	TP1	TP2	TP3	TP4
Connection oriented network	Yes	Yes	Yes	Yes	Yes
Connectionless network	No	No	No	No	Yes
Concatenation and separation	No	Yes	Yes	Yes	Yes
Segmentation and reassembly	Yes	Yes	Yes	Yes	Yes
Error Recovery	No	Yes	No	Yes	Yes
Reinitiate connection (if an excessive number of PDUs are unacknowledged)	No	Yes	No	Yes	No
multiplexing and demultiplexing over a single virtual circuit	No	No	Yes	Yes	Yes
Explicit flow control	No	No	Yes	Yes	Yes
Retransmission on timeout	No	No	No	No	Yes
Reliable Transport Service	No	Yes	No	Yes	Yes

Perhaps an easy way to visualize the Transport Layer is to compare it with a Post Office, which deals with the dispatch and classification of mail and parcels sent. Do remember, however, that a post office manages the outer envelope of mail. Higher layers may have the equivalent of double envelopes, such as cryptographic presentation services that can be read by the addressee only. Roughly speaking, tunneling protocols operate at the Transport Layer, such as carrying non-IP protocols such as IBM's SNA or Novell's IPX over an IP network, or end-to-end encryption with IPsec. While Generic Routing Encapsulation (GRE) might seem to be a Network Layer protocol, if the encapsulation of the payload takes place only at endpoint, GRE becomes closer to a transport protocol that uses IP headers but contains complete frames or packets to deliver to an endpoint. L2TP carries PPP frames inside transport.

Q. Define the Session layer

Session Layer

The Session Layer is Layer 5 of the seven-layer OSI model of computer networking. Communication sessions consist of requests and responses that occur between applications. Session Layer services are commonly used in application environments that make use of remote procedure calls (RPCs). The Session Layer is Layer 5 of the seven-layer OSI model of computer networking. The Session Layer provides the mechanism for opening, closing and managing a session between end-user application processes, i.e. a semi-permanent dialogue.

An example of a Session Layer protocol is the OSI protocol suite Session Layer Protocol, also known as X.225 or ISO 8327. In case of a connection loss this protocol may try to recover the connection. If a connection is not used for a long period, the Session Layer Protocol may close it and re-open it. It provides for either full duplex or half-duplex operation and provides synchronization points in the

stream of exchanged messages.[1] Other examples of Session Layer implementations include Zone Information Protocol (ZIP) – the AppleTalk protocol that coordinates the name binding process, and Session Control Protocol (SCP) – the DECnet Phase IV Session Layer protocol.

Session Layer Services

i. Authentication

ii. Permissions

iii. Session restoration (check pointing and recovery).

Q. List 10 Session Layer protocols.

Session Layer Protocols

1. ADSP, AppleTalk Data Stream Protocol
2. ASP, AppleTalk Session Protocol
3. H.245, Call Control Protocol for Multimedia Communication
4. ISO-SP, OSI Session Layer Protocol (X.225, ISO 8327)
5. iSNS, Internet Storage Name Service
6. L2F, Layer 2 Forwarding Protocol
7. L2TP, Layer 2 Tunneling Protocol
8. NetBIOS, Network Basic Input Output System
9. PAP, Password Authentication Protocol
10. PPTP, Point-to-Point Tunneling Protocol

Q. Compare the Session layer with TCP/IP model.

Comparison with TCP/IP Model

The TCP/IP reference model does not concern itself with the OSI model's details of application or transport protocol semantics and therefore does not consider a Session Layer. OSI's session management in connection with the typical transport protocols (TCP, SCTP), is contained in the Transport Layer protocols, or otherwise considered the realm of the Application Layer protocols. TCP/IP's layers are descriptions of operating scopes (application, host-to-host, network, link) and not detailed prescriptions of operating procedures or data semantics.

Q. Discuss the Presentation Layer

Presentation Layer

The Presentation Layer is the lowest layer at which application programmers consider data structure and presentation, instead of simply sending data in form of datagrams or packets between hosts. This layer deals with issues of string representation - whether they use the Pascal method (an integer length field followed by the specified amount of bytes) or the C/C++ method (null-terminated strings, i.e. "thisisastring\0"). The idea is that the application layer should be able to point at the data to be moved, and the Presentation Layer will deal with the rest.

Encryption is typically done at this level too, although it can be done at the Application, Session, Transport, or Network Layers; each having its own advantages and disadvantages. Another example is representing structure, which is normally standardized at this level, often by using XML. As well as simple pieces of data, like strings, more complicated things are standardized in this layer. Two common examples are 'objects' in object-oriented programming, and the exact way that streaming video is transmitted.

In many widely used applications and protocols, no distinction is made between the presentation and application layers. For example, HTTP, generally regarded as an application layer protocol, has

Presentation Layer aspects such as the ability to identify character encoding for proper conversion, which is then done in the Application Layer.

Within the service layering semantics of the OSI network architecture, the Presentation Layer responds to service requests from the Application Layer and issues service requests to the Session Layer.

Presentation Layer Services

i. Encryption

ii. Compression

Q. Explain CASE and SASE Layer services

Sublayers

The Presentation Layer is composed of two sublayers:

i. CASE (Common Application Service Element)

ii. SASE (Specific Application Service Element)

CASE

The CASE sublayer provides services for the Application Layer and request services from the Presentation Layer. It provides support for common application services, such as:

• ACSE (Association Control Service Element)

• ROSE (Remote Operation Service Element)

• CCR (Commitment Concurrency and Recovery)

• RTSE (Reliable Transfer Service Element)

SASE

The SASE sublayer provides application specific services (protocols), such as

• FTAM (File Transfer, Access and Manager)

• VT (Virtual Terminal)

• MOTIS (Message Oriented Text Interchange Standard)

• CMIP (Common Management Information Protocol)

• JTM (Job Transfer and Manipulation) a former OSI standard

• MMS (Manufacturing Messaging Service)

• RDA (Remote Database Access)

• DTP (Distributed Transaction Processing)

• Tel Net (a remote terminal access protocol)

Q. List Presentation Layer Protocol

Presentation Layer Protocol Examples

1. AFP, Apple Filing Protocol
2. ASCII, American Standard Code for Information Interchange
3. EBCDIC, Extended Binary Coded Decimal Interchange Code
4. ICA, Independent Computing Architecture, the Citrix system core protocol
5. LPP, Lightweight Presentation Protocol
6. NCP, NetWare Core Protocol
7. NDR, Network Data Representation
8. RDP, Remote Desktop Protocol
9. XDR, eXternal Data Representation
10. X.25 PAD, Packet Assembler/Disassembler Protocol

Q. Discuss Application Layer.

Application Layer

The application layer is the OSI layer closest to the end user, which means that both the OSI application layer and the user interact directly with the software application. This layer interacts with software applications that implement a communicating component. Such application programs fall outside the scope of the OSI model. Application layer functions typically include identifying communication partners, determining resource availability, and synchronizing communication. When identifying communication partners, the application layer determines the identity and availability of communication partners for an application with data to transmit. When determining resource availability, the application layer must decide whether sufficient network resources for the requested communication exist. In synchronizing communication, all communication between applications requires cooperation that is managed by the application layer. Some examples of application layer implementations include Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), Simple Mail Transfer Protocol (SMTP) and X.400 Electronic Mail.

Examples

Layer		OSI protocols	TCP/IP Protocols	Signaling System 7	Apple Talk	IPX	SNA	UMTS	Misc. examples
#	Name								
7	Application	FTAM, X.400, X.500, DAP, ROSE, RTSE, ACSE	NNTP, SIP, SSI, DNS, FTP, Gopher, HTTP, DHCP, SMPP, SMTP, SNMP, Telnet, RIP, BGP	INAP, MAP, TCAP, ISUP, TUP	AFP, ZIP, RTMP, NBP	RIP SAP	APPC		HL7, Modbus

Q. Discuss the TCP/IP model

The TCP/IP Model

The TCP/IP model or Internet reference model, sometimes called the DoD [(Department of Defense) model or the ARPANET reference model, is a layered abstract description for communications and computer network protocol design. It was created in the 1970s by DARPA for use in developing the Internet's protocols. It is a suite of protocols among which TCP and IP are the two main protocols, hence the name. This model was developed before the OSI Reference Model, and the Internet

Engineering Task Force (IETF), which is responsible for the model and protocols developed under it, has never felt obligated to be compliant with OSI.

The model is composed of 5 layers

1. Physical
2. Data Link
3. Network
4. Transport
5. Application

The TCP/IP Advantage

The reasons that TCP/IP has become the most widely used protocol are as follows:

1. The flexible addressing scheme of TCP/IP allows data to be routed over even very large networks.
2. Virtually all operating systems and platforms can use TCP/IP.
3. TCP/IP offers a very large number of utilities and tools.
4. The I/internet communication is based on TCP/IP.

Q. Outline TCP/IP Services and Protocols

TCP/IP Services and Protocols

Layer	Services	Protocols	Devices
Physical Layer	• Dictates Signal Characteristics • Data Transmission • Signal Multiplexing • Dictates Network L/O • Dictates Media Characteristics • Switching	• HSSI • X.21	• Repeaters • Hubs • Modems
Data Link Layer	• Error Detection and Correction • Flow and Error Control • Media Access Control • Virtual Circuit Switching	• HDLC • ARP/RARP • SLIP • PPP	• Bridges • Switches

Network Layer	• Internetworking
	• Logical Addressing
	• Routing
	• Datagram Switching
		• Routed Protocols
		  ○ IGMP
		  ○ IP
		  ○ ICMP
		• Routing
		  ○ OSF
			• Routers
			• Gateways

Transport Layer	• Process-to-Process Delivery • Congestion Control • Quality of Service	• TCP • UDP	N/A
Application Layer	• WWW • Mail • Multimedia	• TFTP • HTTP • FTP • SMTP • SNMP • POP3	• Application Gateways

Q. Discuss the Internet Protocol (IP).

The Internet Protocol (IP)

The IP component of TCP/IP determines where packets of data are to be routed based on their destination addresses, and IP has certain characteristics related to how it handles this function. The functioning of an IP based communication is analogous to Delivering Mail Through the Postal Service.

IP Characteristics

1. Operates at network layer
2. Connectionless protocol- The destination device receives the data and does not return any status information to the sending device
3. Packets treated independently- A packet can be misdirected, duplicated, or lost on the way to its destination.
4. Hierarchical addressing
5. Best-effort delivery
6. No data recovery features- does not provide any special features that recover corrupted packets

IP Packet Format

• The header consists of 12 fields + 1 optional field

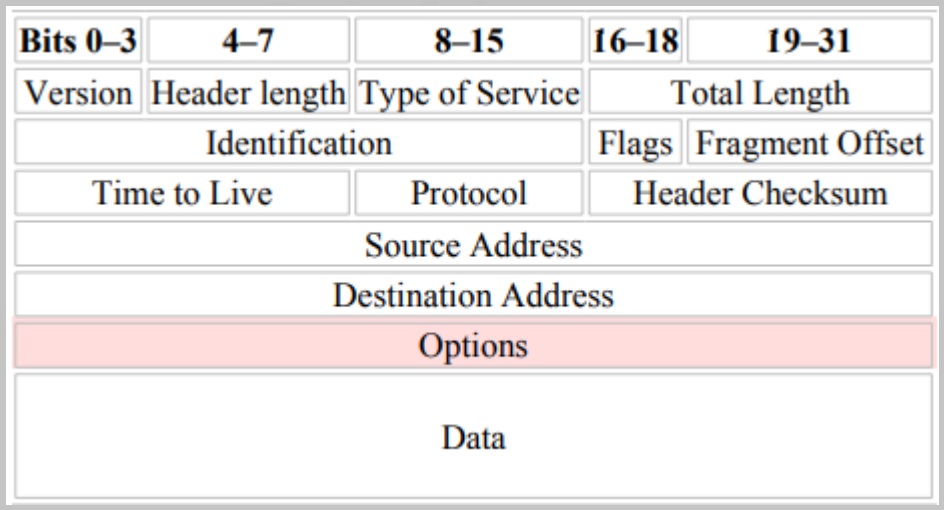
• Version(4bits) :For IPv4, this has a value of 4 (hence the name IPv4).

• Internet Header Length(4bits) : tells the number of 32-bit words in the header. In IPv4, this field specifies the size of the header.

• Type of Service (8bits)

o bits 0-2: precedence

o bit 3: 0 = Normal Delay, 1 = Low Delay



o bit 4:

0 = Normal Throughput, 1 = High Throughput

o bit 5: 0 = Normal Reliability, 1 = High Reliability

o bits 6-7: Reserved for future use or for Differentiated services or for Explicit Congestion Notification

• Total Length(16bits) : defines the entire datagram size, including header and data, in bytes.

• Identification : primarily used for uniquely identifying fragments of an original IP datagram.

• Flags(3bits) : used to control or identify fragments. They are (in order, from high order to low order):

o Reserved; must be zero.

o Don't Fragment (DF)

o More Fragments (MF)

• Fragment Offset(13bits) : specifies the offset of a particular fragment relative to the beginning of the original unfragmented IP datagram.

• Time To Live (8bits): helps prevent datagrams from persisting in an internetwork. When the TTL field hits zero, the packet is no longer forwarded by a packet switch and is discarded.

• Protocol: defines the protocol used in the data portion of the IP datagram.

• Header Checksum (16bits): used for error-checking of the header.

• Source address: An IP address is a group of 4, 8-bit octets for a total of 32 bits. The value for this field is determined by taking the binary value of each octet and concatenating them together to make a single 32-bit value.

• Destination address: indicates the address of the packet receiver.

• Options: Additional header fields may follow the destination address field, but these are not often used. Note that the value in the IHL field must include enough extra 32-bit words to hold all the options (plus any padding needed to ensure that the header contains an integral number of 32-bit words)

IP Addressing

• Each IP address has specific components and follows a basic format. These IP addresses can be subdivided and used to create addresses for subnetwork.

• Each host on a TCP/IP network is assigned a unique 32-bit logical address that is divided into two main parts:

o the network number- identifies a network, assigned by InterNIC or an ISP

o the host number-identifies a host on a network, assigned by the local network administrator.

• IPv4 Address representations

Notation	Value	Conversion from dot-decimal
Dot-decimal notation	192.0.2.235	N/A
Dotted Hexadecimal	0xC0.0x00.0x02.0xEB	Each octet is individually converted to hex
Dotted Octal	0300.0000.0002.0353	Each octet is individually converted into octal
Hexadecimal	0xC00002EB	Concatenation of the octets from the dotted hexadecimal
Decimal	3221226219	The hexadecimal form converted to decimal
Octal	030000001353	The hexadecimal form converted to octal

• IP Address Classes

o The IPV4 addresses are divided into five different address classes: A, B,C, D, and E.

Q. Explain Analog Signal processing

Analog Signal Processing

Analog signal processing is any signal processing conducted on analog signals by analog means. "Analog" indicates something that is mathematically represented as a set of continuous values. This differs from "digital" which uses a series of discrete quantities to represent signal. Analog values are typically represented as a voltage, electric current, or electric charge around components in the electronic devices. An error or noise affecting such physical quantities will result in a corresponding error in the signals represented by such physical quantities. Examples of analog signal processing include crossover filters in loudspeakers, "bass", "treble" and "volume" controls on stereos, and "tint" controls on TVs. Common analog processing elements include capacitors, resistors, inductors and transistors.

Q. Discus tools used in analog signal processing

Tools Used in Analog Signal Processing

A system's behavior can be mathematically modeled and is represented in the time domain as h(t) and in the frequency domain as H(s), where s is a complex number in the form of s = a+ib, or s = a+jb in electrical engineering terms (electrical engineers use j because current is represented by the variable i). Input signals are usually called x(t) or X(s) and output signals are usually called y(t) or Y(s).

1. Convolution

nal can be combined with the system's function to find the output signal. It is the integral of the product of two waveforms after one has reversed and shifted; the symbol for convolution is *.

$$y(t) = (x * h)(t) = \int_a^b x(\tau)h(t-\tau)\,d\tau$$

That is the convolution integral and is used to find the convolution of a signal and a system; typically a = -∞ and b = +∞. Consider two waveforms f and g. By calculating the convolution, we determine how much a reversed function g must be shifted along the xaxis to become identical to function f. The convolution function essentially reverses and slides function g along the axis, and calculates the integral of their (f and the reversed and shifted g) product for each possible amount of sliding. When the functions match, the value of (f*g) is maximized. This occurs because when positive areas (peaks) or negative areas (troughs) are multiplied, they contribute to the integral.

2. Fourier transform

The Fourier transform is a function that transforms a signal or system in the time domain into the frequency domain, but it only works for certain ones. The constraint on which systems or signals can be transformed by the Fourier Transform is that:

$$\int_{-\infty}^{\infty} |x(t)|\,dt < \infty$$

This is the Fourier transform integral:

$$X(j\omega) = \int_{-\infty}^{\infty} x(t)e^{-j\omega t}\,dt$$

Most of the time the Fourier transform integral isn't used to determine the transform. Usually a table of transform pairs is used to find the Fourier transform of a signal or system. The inverse Fourier transform is used to go from frequency domain to time domain:

$$x(t) = \frac{1}{2\pi}\int_{-\infty}^{\infty} X(j\omega)e^{j\omega t}\,d\omega$$

Each signal or system that can be transformed has a unique Fourier transform; there is only one time signal and one frequency signal that goes together.

3. Laplace transform

The Laplace transform is a generalized Fourier transform. It allows a transform of any system or signal because it is a transform into the complex plane instead of just the jω line like the Fourier transform. The major difference is that the Laplace transform has a region of convergence for which the transform is valid. This implies that a signalin frequency may have more than one signal in time; the correct time signal for the transform is determined by the region of convergence. If the region of convergence includes the jω axis, jω can be substituted into the Laplace transform for s and it's the same as the Fourier transform. The Laplace transform is:

$$X(s) = \int_{-\infty}^{\infty} x(t)e^{-st}\,dt$$

and the inverse Laplace transform is:

$$x(t) = \frac{1}{2\pi}\int_{-\infty}^{\infty} X(s)e^{st}\,ds$$

4. Bode plots

Bode plots are plots of magnitude vs. frequency and phase vs. frequency for a system. The magnitude axis is in Decibel (dB). The phase axis is in either degrees or radians. The frequency axes are in a logarithmic scale. These are useful because for sinusoidal inputs, the output is the input multiplied by

the value of the magnitude plot at the frequency and shifted by the value of the phase plot at the frequency.

Q. Discuss Domains

Domains

1. Time domain

This is the domain that most people are familiar with. A plot in the time domain shows the magnitude of a signal at a point in time.

2. Frequency domain

This is the domain that engineers are glad exists. It's unfamiliar to most people, but makes the math associated with analog signal processing much easier than if it's analyzed in the time domain. A plot in the frequency domain shows either the phase shift or magnitude of a signal at each frequency that it exists at. These can be found by taking the Fourier transform of a time signal and are plotted similarly to a bode plot.

Q. Explain Signals

Signals

While any signal can be used in analog signal processing, there are many types of signals that are used very frequently.

i. Sinusoids

Sinusoids are the building block of analog signal processing. Theorem states that all real world signals can be represented by a sum of sinusoids. A sinusoid can be represented by a complex exponential, e^{st}.

ii. Impulse

An impulse (Dirac delta function) is defined as a signal that has an infinite magnitude and an infinitesimally narrow width with an area under it of one, centered at zero. An impulse can be represented as an infinite sum of sinusoids that includes all possible frequencies. It is not, in reality, possible to generate such a signal, but it can be sufficiently approximated with a large amplitude, narrow pulse, to produce the theoretical impulse response in a network to a high degree of accuracy. The symbol for an impulse is δ(t). If an impulse is used as an input to a system, the output is known as the impulse response. The impulse response defines the sy

iii. Step

A unit step function, also called the Heaviside step function, is a signal that has a magnitude of zero before zero and a magnitude of one after zero. The symbol for a unit step is u(t). If a step is used as the input to a system, the output is called the step response. The step response shows how a system responds to a sudden input, similar to turning on a switch. The period before the output stabilizes is called the transient part of a signal. The step response can be multiplied with other signals to show how the system responds when an input is suddenly turned on. The unit step function is related to the Dirac delta function by;

$$\mathrm{u}(t) = \int \delta(t).dt$$

Q. Discuss Systems

Systems

1. Linear time-invariant (LTI)

Linearity means that if you have two inputs and two corresponding outputs, if you take a linear combination of those two inputs you will get a linear combination of the outputs. An example of a linear system is a first order low-pass or high-pass filter. Linear systems are made out of analog devices that demonstrate linear properties. These devices don't have to be entirely linear, but must have a region of operation that is linear. An operational amplifier is a non-linear device, but has a region of operation that is linear, so it can be modeled as linear within that region of operation. Time-invariance means it doesn't matter when you start a system, the same output will result. For example, if you have a system and put an input into it today, you would get the same output if you started the system tomorrow instead. There aren't any real systems that are LTI, but many systems can be modeled as LTI for simplicity in determining what their output will be. All systems have some dependence on things like temperature, signal level or other factors that cause them to be non-linear or non-time-invariant, but most are stable enough to model as LTI. Linearity and time-invariance are important because they are the only types of systems that can be easily solved using conventional analog signal processing methods. Once a system becomes non-linear or non-time-invariant, it becomes a non-linear differential equations problem, and there are very few of those that can actually be solved.

2. Common systems

Some common systems used in everyday life are filters, AM/FM radio, electric guitars and musical instrument amplifiers. Filters are used in almost everything that has electronic circuitry. Radio and television are good examples of everyday uses of filters. When a channel is changed on an analog television set or radio, an analog filter is used to pick out the carrier frequency on the input signal. Once it's isolated, the television or radio information being broadcast is used to form the picture and/or sound. Another common analog system is an electric guitar and its amplifier. The guitar uses a magnet with a coil wrapped around it (inductor) to turn the vibration of the strings into a small electric current. The current is then filtered, amplified and sent to a speaker in the amplifier. Most amplifiers are analog because they are easier and cheaper to make than making a digital amplifier. There are also many analog guitar effects pedals, although a large number of pedals are now digital (they turn the input current into a digitized value, perform an operation on it, then convert it back into an analog signal).

Q. Explain Digital Signal Processing

Digital Signal Processing

Digital signal processing (DSP) is concerned with the representation of the signals by a sequence of numbers or symbols and the processing of these signals. Digital signal processing and analog signal processing are subfields of signal processing. DSP includes subfields like: audio and speech signal processing, sonar and radar signal processing, sensor array processing, spectral estimation, statistical signal processing, digital image processing, signal processing for communications, biomedical signal processing, seismic data processing, etc.

Since the goal of DSP is usually to measure or filter continuous realworld analog signals, the first step is usually to convert the signal from an analog to a digital form, by using an analog to digital converter. Often, the required output signal is another analog output signal, which requires a digital to analog converter. Even if this process is more complex than analog processing and has a discrete value range, the stability of digital signal processing thanks to error detection and correction and being less vulnerable to noise makes it advantageous over analog signal processing for many, though not all, applications.

DSP algorithms have long been run on standard computers, on specialized processors called digital signal processors (DSPs), or on purpose-built hardware such as application-specific integrated circuit

(ASICs). Today there are additional technologies used for digital signal processing including more powerful general purpose microprocessors, field-programmable gate arrays (FPGAs), digital signal controllers (mostly for industrial apps such as motor control), and stream processors, among others.

Q. Explain Digital Signal Domain

DSP Domains

In DSP, engineers usually study digital signals in one of the following domains: time domain (one-dimensional signals), spatial domain (multidimensional signals), frequency domain, autocorrelation domain, and wavelet domains. They choose the domain in which to process a signal by making an informed guess (or by trying different possibilities) as to which domain best represents the essential characteristics of the signal. A sequence of samples from a measuring device produces a time or spatial domain representation, whereas a discrete Fourier transform produces the frequency domain information, that is the frequency spectrum. Autocorrelation is defined as the cross-correlation of the signal with itself over varying intervals of time or space.

Q. Discuss Signal sampling

Signal Sampling

With the increasing use of computers the usage of and need for digital signal processing has increased. In order to use an analog signal on a computer it must be digitized with an analog to digital converter (ADC). Sampling is usually carried out in two stages, discretization and quantization. In the discretization stage, the space of signals is partitioned into equivalence classes and quantization is carried out by replacing the signal with representative signal of the corresponding equivalence class. In the quantization stage the representative signal values are approximated by values from a finite set. The Nyquist–Shannon sampling theorem states that a signal can be exactly reconstructed from its samples if the sampling frequency is greater than twice the highest frequency of the signal. In practice, the sampling frequency is often significantly more than twice the required bandwidth. A digital to analog converter (DAC) is used to convert the digital signal back to analog. The use of a digital computer is a key ingredient in digital control systems.

Q. Discuss Time and Space Domains

Time and Space Domains

The most common processing approach in the time or space domain is enhancement of the input signal through a method called filtering. Filtering generally consists of some transformation of a number of surrounding samples around the current sample of the input or output signal. There are various ways to characterize filters; for example:

• A "linear" filter is a linear transformation of input samples; other filters are "non-linear." Linear filters satisfy the superposition condition, i.e. if an input is a weighted linear combination of different signals, the output is an equally weighted linear combination of the corresponding output signals.

• A "causal" filter uses only previous samples of the input or output signals; while a "non-causal" filter uses future input samples. A non-causal filter can usually be changed into a causal filter by adding a delay to it.

• A "time-invariant" filter has constant properties over time; other filters such as adaptive filters change in time.

• Some filters are "stable", others are "unstable". A stable filter produces an output that converges to a constant value with time, or remains bounded within a finite interval. An unstable filter can produce an output that grows without bounds, with bounded or even zero input.

• A "finite impulse response" (FIR) filter uses only the input signal, while an "infinite impulse response" filter (IIR) uses both the input signal and previous samples of the output signal. FIR filters are always stable, while IIR filters may be unstable.

Q. Explain Frequency Domain

Frequency Domain

Signals are converted from time or space domain to the frequency domain usually through the Fourier transform. The Fourier transform converts the signal information to a magnitude and phase component of each frequency. Often the Fourier transform is converted to the power spectrum, which is the magnitude of each frequency component squared. The most common purpose for analysis of signals in the frequency domain is analysis of signal properties. The engineer can study the spectrum to determine which frequencies are present in the input signal and which are missing. Frequency domain analysis is also called spectrum- or spectral analysis.

Q. List the techniques involved in Digital Signal Processing

Techniques Involved in Digital Signal Processing

1. Bilinear transform
2. Discrete Fourier transform
3. Discrete-time Fourier transform
4. Filter design
5. LTI system theory
6. Minimum phase
7. Transfer function
8. Z-transform
9. Goertzel algorithm
10. s-plane

Q. What is networking?

Networking

Networking is a complex part of computing that makes up most of the IT Industry. Without networks, almost all communication in the world would cease to happen. It is because of networking that telephones, televisions, the Computer networking devices are units that mediate data in a computer network.. Computer networking devices are also called network equipment, Intermediate Systems (IS) or InterWorking Unit (IWU). Units which are the last receiver or generate data are called hosts or data terminal equipment internet, etc. work.

Networking Methods

One way to categorize computer networks is by their geographic scope, although many real-world networks interconnect Local Area Networks (LAN) via Wide Area Networks (WAN) and wireless networks [WWAN]. These three (broad) types are:

1. Local Area Network (LAN)

A local area network is a network that spans a relatively small space and provides services to a small number of people. A peer-to-peer or client-server method of networking may be used. A peer-to-peer network is where each client shares their resources with other workstations in the network. Examples of peer-to-peer networks are: Small office networks where resource use is minimal and a home network. A client-server network is where every client is connected to the server and each other. Client-server networks use servers in different capacities. These can be classified into two types:

1. Single-service servers

2. Print server

2. Wide Area Network (WAN)

A wide area network is a network where a wide variety of resources are deployed across a large domestic area or internationally. An example of this is a multinational business that uses a WAN to interconnect their offices in different countries. The largest and best example of a WAN is the Internet, which is a network composed of many smaller networks. The Internet is considered the largest network in the world. The PSTN (Public Switched Telephone Network) also is an extremely large network that is converging to use Internet technologies, although not necessarily through the public Internet.

A Wide Area Network involves communication through the use of a wide range of different technologies. These technologies include Pointto-Point WANs such as Point-to-Point Protocol (PPP) and High-Level Data Link Control (HDLC), Frame Relay, ATM (Asynchronous Transfer Mode) and Sonet (Synchronous Optical Network). The difference between the WAN technologies is based on the switching capabilities they perform and the speed at which sending and receiving bits of information (data) occur.

3. Metropolitan Area Network (MAN)

A metropolitan network is a network that is too large for even the largest of LAN's but is not on the scale of a WAN. It also integrates two or more LAN networks over a specific geographical area (usually a city) so as to increase the network and the flow of communications. The LAN's in question would usually be connected via "backbone" lines.

4. Wireless Networks (WLAN, WWAN)

A wireless network is basically the same as a LAN or a WAN but there are no wires between hosts and servers. The data is transferred over sets of radio transceivers. These types of networks are beneficial when it is too costly or inconvenient to run the necessary cables. For more information, see Wireless LAN and Wireless wide area network. The media access protocols for LANs come from the IEEE. The most common IEEE 802.11 WLANs cover, depending on antennas, ranges from hundreds of meters to a few kilometers.

Q. List and define five Common Basic Networking Devices

Common Basic Networking Devices

i. Gateway: device sitting at a network node for interfacing with another network that uses different protocols. Works on OSI layers 4 to 7.

ii. Router: a specialized network device that determines the next network point to which to forward a data packet toward its destination. Unlike a gateway, it cannot interface different protocols. Works on OSI layer 3.

iii. Bridge: a device that connects multiple network segments along the data link layer. Works on OSI layer 2.

iv. Switch: a device that allocates traffic from one network segment to certain lines (intended destination(s)) which connect the segment to another network segment.

v. Hub: connects multiple Ethernet segments together making them act as a single segment. When using a hub, every attached device shares the same broadcast domain and the same collision domain.

vi. Repeater: device to amplify or regenerate digital signals received while setting them from one part of a network into another. Works on OSI layer 1.

Hybrid Network Devices

i. Multilayer Switch: a switch which, in addition to switching on OSI layer 2, provides functionality at higher protocol layers.

ii. Protocol Converter: a hardware device that converts between two different types of transmissions, such as asynchronous and synchronous transmissions.

iii. Bridge Router (Brouter): Combine router and bridge functionality and are therefore working on OSI layers 2 and 3.

iv. Digital media receiver: Connects a computer network to a home theatre

Software for Networks or Dial-up Connections

i. Proxy: computer network service which allows clients to make indirect network connections to other network services

ii. Firewall: a piece of hardware or software put on the network to prevent some communications forbidden by the network policy

iii. Network Address Translator: network service provide as hardware or software that converts internal to external network addresses and vice versa

Other Hardware for Networks or Dial-up Connections

i. Multiplexer: device that combines several electrical signals into a single signal

ii. Network Card: a piece of computer hardware to allow the attached computer to communicate by network

iii. Modem: device that modulates an analog "carrier" signal (such as sound), to encode digital information, and that also demodulates such a carrier signal to decode the transmitted information, as a computer communicating with another computer over the telephone network

iv. ISDN terminal adapter (TA): a specialized gateway for ISDN

v. Line Driver: a device to increase transmission distance by amplifying the signal. Base-band networks only.

Q. What is Network Topology?

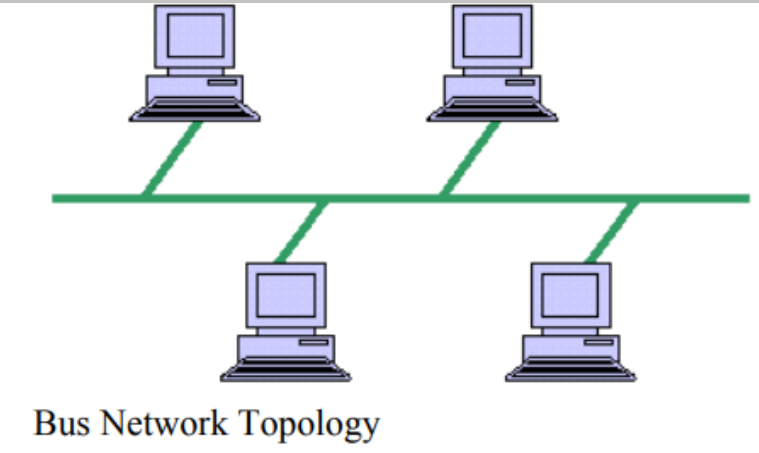
Network Topology

The network topology defines the way in which computers, printers, and other devices are connected, physically and logically. A network topology describes the layout of the wire and devices as well as the paths used by data transmissions.

Q. Explain Bus, Ring, Star, Tree and mesh network Topologies.

1. Bus Topology

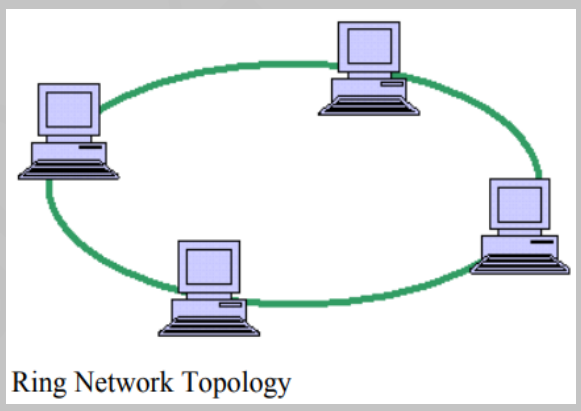
Bus networks (not to be confused with the system bus of a computer) use a common backbone to connect all devices. A single cable, the backbone functions as a shared communication medium that devices attach or tap into with an interface connector. A device wanting to communicate with another device on the network sends a broadcast message onto the wire that all other devices see, but only the intended recipient actually accepts and processes the message.



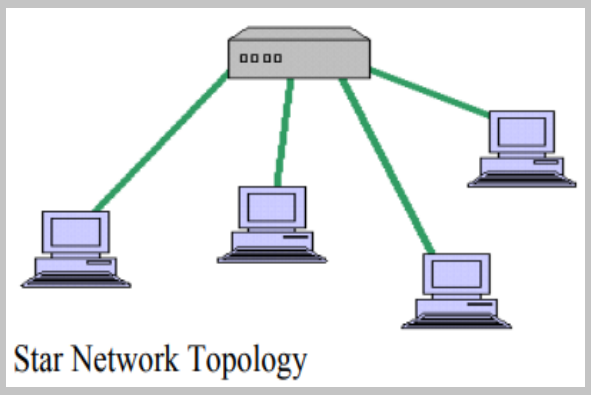
Ethernet bus topologies are relatively easy to install and don't require much cabling compared to the alternatives. 10Base-2 ("ThinNet") and 10Base-5 ("ThickNet") both were popular Ethernet cabling options many years ago for bus topologies. However, bus networks work best with a limited number of devices. If more than a few dozen computers are added to a network bus, performance problems will likely result. In addition, if the backbone cable fails, the entire network effectively becomes unusable.

2. Ring Topology

In a ring network, every device has exactly two neighbors for communication purposes. All messages travel through a ring in the same direction (either "clockwise" or "counterclockwise"). A failure in any cable or device breaks the loop and can take down the entire network. To implement a ring network, one typically uses FDDI, SONET, or Token Ring technology. Ring topologies are found in some office buildings or school campuses. This diagram illustrates the ring network topology. A ring topology such as FDDI or SONET sends messages clockwise or counterclockwise through the shared link.



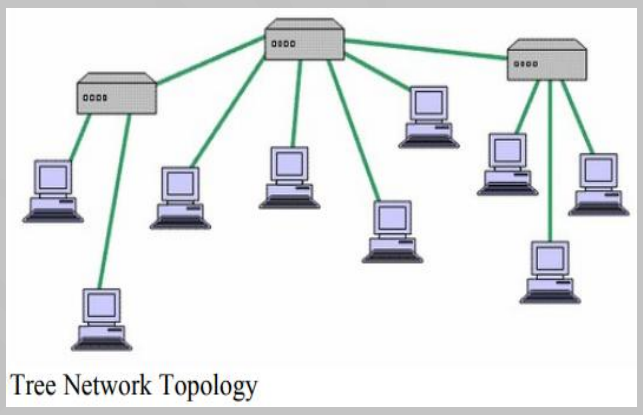
3. Star Topology



Many home networks use the star topology. A star network features a central connection point called a "hub" that may be a hub, switch or router. Devices typically connect to the hub with Unshielded Twisted Pair (UTP) Ethernet. Compared to the bus topology, a star network generally requires more cable, but a failure in any star network cable will only take down one computer's network access and not the entire LAN. (If the hub fails, however, the entire network also fails.) This diagram illustrates the star network topology. A star topology typically uses a network hub or switch and is common in home networks.

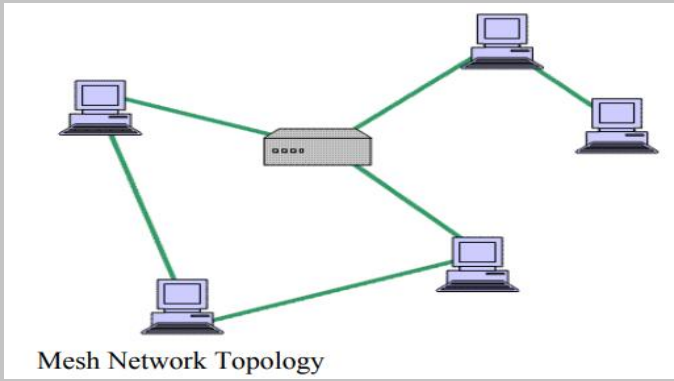
4. Tree Topology

Tree topologies integrate multiple star topologies together onto a bus. In its simplest form, only hub devices connect directly to the tree bus, and each hub functions as the "root" of a tree of devices. This bus/star hybrid approach supports future expandability of the network much better than a bus (limited in the number of devices due to the broadcast traffic it generates) or a star (limited by the number of hub connection points) alone. This diagram illustrates the tree network topology. A tree topology integrates the star and bus topologies in a hybrid approach to improve network scalability.



5. Mesh Topology

Mesh topologies involve the concept of routes. Unlike each of the previous topologies, messages sent on a mesh network can take any of several possible paths from source to destination. (Recall that even in a ring, although two cable paths exist, messages can only travel in one direction.) Some WANs, most notably the Internet, employ mesh routing. A mesh network in which every device connects to every other is called a full mesh. As shown in the illustration below, partial mesh networks also exist in which some devices connect only indirectly to others. This diagram illustrates the mesh network topology. A mesh topology provides redundant communication paths between some or all devices (partial or full mesh).



Mesh Network Topology

Q. Discourse Internet Telephony

Internet Telephony

Internet telephony refers to communications services—voice, facsimile, and/or voice-messaging applications—that are transported via the Internet, rather than the public switched telephone network (PSTN). The basic steps involved in originating an Internet telephone call are conversion of the analog voice signal to digital format and compression/ translation of the signal into Internet protocol (IP) packets for transmission over the Internet; the process is reversed at the receiving end. Internet telephony within an intranet enables users to save on long distance bills between sites; they can make point-to-point calls via gateway servers attached to the local-area network (LAN). No PC–based telephony software or Internet account is required.

Q. Explain the Technical Barriers in VOIP

Technical Barriers

The ultimate objective of Internet telephony is, of course, reliable, high quality voice service, the kind that users expect from the PSTN. At the moment, however, that level of reliability and sound quality is not available on the Internet, primarily because of bandwidth limitations that lead to packet loss. In voice communications, packet loss shows up in the form of gaps or periods of silence in the conversation, leading to a clipped-speech effect that is unsatisfactory for most users and unacceptable in business communications.

The Internet, a collection of more than 130,000 networks, is gaining in popularity as millions of new users sign on every month. The increasingly heavy use of the Internet's limited bandwidth often results in congestion which, in turn, can cause delays in packet transmission. Such network delays mean packets are lost or discarded. The lack of standardized protocols also means that many Internet-telephony products do not interoperate with each other or with the PSTN.

Q. Discuss the future of VOIP

Future VoIP

Several factors will influence future developments in VoIP products and services. Currently, the most promising areas for VoIP are corporate intranets and commercial extranets. Their IP–based infrastructures enable operators to control who can—and cannot—use the network. Another influential element in the ongoing Internet-telephony evolution is the VoIP gateway. As these gateways evolve from PC–based platforms to robust embedded systems, each will be able to handle hundreds of simultaneous calls. Consequently, corporations will deploy large numbers of them in an effort to reduce the expenses associated with high-volume voice, fax, and videoconferencing traffic. The economics of placing all traffic— data, voice, and video—over an IP– based network will pull companies in this direction, simply because IP will act as a unifying agent, regardless of the underlying architecture (i.e., leased lines, frame relay, or ATM) of an organization's network.

Commercial extranets, based on conservatively engineered IP networks, will deliver VoIP and facsimile over Internet protocol (FAXoIP) services to the general public. By guaranteeing specific parameters, such as packet delay, packet jitter, and service interoperability, these extranets will ensure reliable network support for such applications.

VoIP products and services transported via the public Internet will be niche markets that can tolerate the varying performance levels of that transport medium. Telecommunications carriers most likely will rely on the public Internet to provide telephone service between/among geographic locations that today are high-tariff areas. It is unlikely that the public Internet's performance characteristics will improve sufficiently within the next two years to stimulate significant growth in VoIP for that medium.

Q. Explain guided media of communication

Guided Media of Communication

Guided media, which are those that provide a conduit from one device to another, include twisted-pair cable, coaxial cable, and fiber-optic cable. A signal traveling along any of these media is directed and contained by the physical limits of the medium. Twisted-pair and coaxial cable use metallic (copper) conductors that accept and transport signals in the form of electric current. Optical fiber is a cable that accepts and transports signals in the form of light.

Q. List and discuss three guided Media.

1. Twisted-Pair Cable

A twist pair consists of two conductors (normally copper), each with its own plastic insulation, twisted together as shown in figure 7.3. One of the wires is used to carry signals to the receiver, and the other is used only as a ground reference. The receiver uses the difference between the two. In addition to the signal sent by the sender on one of the wires, interference (muse) and crosstalk may affect both wires and create unwanted signals.

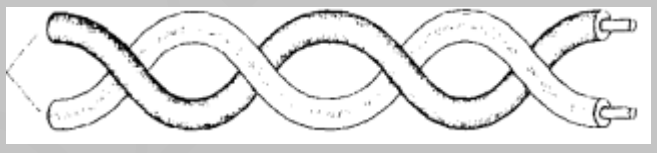


Figure 7.3 Twisted-pair cable

2. Coaxial Cable

Coaxial cable (or coax) carries signals of higher frequency ranges than those in twisted pair cable, in part because the two media are constructed quite differently. Instead of having two wires, coax has a central core conductor of solid or stranded wire (usually copper) enclosed in an insulating sheath, which is, in turn, encased in an outer conductor of metal foil, braid, or a combination of the two. The outer metallic wrapping serves both as a shield against noise and as the second conductor, which completes the circuit. This outer conductor is also enclosed in an insulating sheath, and the whole cable is protected by a plastic cover.

Figure 7.7 Coaxial cable

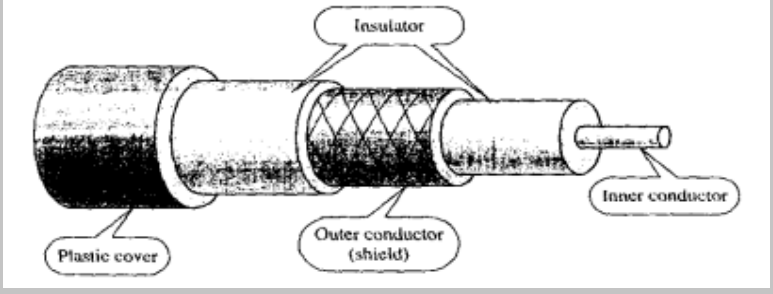


Table 7.2 Categories of coaxial cables

Category	*Impedance*	*Use*
RG-59	75	Cable TV
RG-58	50	Thin Ethernet
RG-11	50	Thick Ethernet

3. Fiber-Optic Cable

A fiber-optic cable is made of glass or plastic and transmits signals in the form of light. To understand optical fiber, we first need to explore several aspects of the nature of light. Light travels in a straight line as long as it is moving through a single uniform substance. If a ray of light traveling through one substance suddenly enters another substance (of a different density), the ray changes direction. Optical fibers use reflection to guide light through a channel. Fiber-optic cable is often found in backbone networks because its wide bandwidth is cost-effective.

Advantages of Optical Fiber

1. Higher bandwidth
2. Less signal attenuation
3. Immunity to electromagnetic interference.
4. Resistance to corrosive materials.
5. Light weight.
6. Greater immunity to tapping.

Disadvantages of Optical Fiber

1. Installation and maintenance.
2. Unidirectional light propagation.
3. Cost

Q. Discuss unguided media of network communication

Unguided Media of Network Communication

Unguided media transport electromagnetic waves without using a physical conductor. This type o f communication is often referred to as wireless communication. Signals are normally broadcast through free space and thus are available to anyone who has a device capable of receiving them. Unguided signals can travel from the source to destination in several ways: ground propagation, sky propagation, and line-of-sight propagation. In ground propagation, radio waves travel through the lowest portion of the atmosphere, hugging the earth. These low-frequency signals emanate in all directions from the transmitting antenna and follow the curvature of the planet. Distance depends on the amount of power in the signal: The greater the power, the greater the distance. In sky propagation, higher-frequency radio waves radiate upward into the ionosphere (the layer of atmosphere where particles exist as ions) where they are reflected back to earth. This type of transmission allows for

greater distances with lower output power. In line-of-sight propagation, very high-frequency signals are transmitted in straight lines directly from antenna to antenna. Antennas must be directional, facing each other and either tall enough or close enough together not to be affected by the curvature of the earth. Line-of-sight propagation is tricky because radio transmissions cannot be completely focused.

Q. Explain Radio waves, Microwaves and Infrared

1. Radio Waves

Although there is no clear-cut demarcation between radio waves and microwaves, electromagnetic waves ranging in frequencies between 3 kHz and 1 GHz are normally called radio waves; waves ranging in frequencies between 1 and 300 GHz are called microwaves. However, the behavior of the waves, rather than the frequencies, is a better criterion for classification. Radio waves use omnidirectional antennas that send out signals in all directions. Based on the wavelength, strength, and the purpose of transmission, we can have several types of antennas. The omnidirectional characteristics of radio waves make them useful for multicasting, in which there is one sender but many receivers. AM and FM radio, television, maritime radio, cordless phones, and paging are examples of multicasting.

2. Microwaves

Electromagnetic waves having frequencies between 1 and 300 GHz are called microwaves. Microwaves are unidirectional. When an antenna transmits microwave waves, they can be narrowly focused. This means that the sending and receiving antennas need to be aligned. The unidirectional property has an obvious advantage. A pair of antennas can be aligned without interfering with another pair of aligned antennas. Microwaves need unidirectional antennas that send out signals in one direction. Two types of antennas are used for microwave communications: the parabolic dish and the horn.

The following describes some characteristics of microwave propagation:

1. Microwave propagation is line-of-sight.
2. Very high-frequency microwaves cannot penetrate walls.
3. The microwave band is relatively wide, almost 299 GHz.
4. Use of certain portions of the band requires permission from authorities.

3. Infrared

Infrared waves, with frequencies from 300 GHz to 400 THz (wavelengths from I mm to 770 nm), can be used for short-range communication. Infrared waves, having high frequencies, cannot penetrate walls. This advantageous characteristic prevents interference between one system and another; a short-range communication system in one room cannot be affected by another system in the next room. When we use our infrared remote control, we do not interfere with the use of the remote by our neighbors. However, this same characteristic makes infrared signals useless for long-range communication. In addition, we cannot use infrared waves outside a building because the sun's rays contain infrared waves that can interfere with the communication.

Q. Discuss briefly Transmission impairment

Transmission Impairment

Signals travel through transmission media, which are not perfect. The imperfection causes signal impairment. This means that the signal at the beginning of the medium is not the same as the signal at the end of the medium. What is sent is not what is received. Three causes of impairment are attenuation, distortion, and noise

Q. What is attenuation?

Attenuation

Attenuation means a loss of energy. When a signal, simple or composite, travels through a medium, it loses some of its energy in overcoming the resistance of the medium. That is why a wire carrying electric signals gets warm, if not hot, after a while. Some of the electrical energy in the signal is converted to heat. To compensate for this loss, amplifiers are used to amplify the signal.

Q. Explain Distortion?

Distortion

Distortion means that the signal changes its form or shape. Distortion can occur in a composite signal made of different frequencies. Each signal component has its own propagation speed (see the next section) through a medium and, therefore, its own delay in arriving at the final destination. Differences in delay may create a difference in phase if the delay is not exactly the same as the period duration. In other words, signal components at the receiver have phases different from what they had at the sender. The shape of the composite signal is therefore not the same.

Q. What is Signal- to- Noise Ratio (SNR)?

Signal- to- Noise Ratio (SNR)

SNR is actually the ratio of what is wanted (signal) to what is not wanted (noise). A high SNR means the signal is less corrupted by noise; a low SNR means the signal is more corrupted by noise. Because SNR is the ratio of two powers, it is often described in decibel units, SNRdB, defined as:

$$SNRdB = 10\log_{10}SNR$$

Q. What is Decibel?

Decibel

To show that a signal has lost or gained strength, engineers use the unit of the decibel. The decibel (dB) measures the relative strengths of two signals or one signal at two different points. Note that the decibel is negative if a signal is attenuated and positive if a signal is amplified.

Q. What is a Network Operating System (NOS)?

Network Operating System (NOS)

A Network Operating System (NOS) transfers files between computers, and between computers and print servers. Often when a user is using a program, such as a word processor, and requests a file, the user is not aware that the file was not residing on his or her machine's hard drive. A Network Operating System (NOS) transfers files between computers, and between computers and print servers. The NOS monitors who logs in and that the user employs the correct password. The latest NOS versions have elaborate methods of hacker/intruder detection, monitoring, and disabling the hacker.

Q. Compare a Computer with a NOS to a Computer without a NOS and a Network Interface Card (NIC)

PC with Network Operating Systems

When a NOS is added to a computer, a major addition is the Redirector as shown in fig 6.1.When the Redirector receives a command from the application program, the Redirector determines if the command is intended for the computer Operating System (OS) and BIOS, or for the network. If the command is a network command, it will be directed to the LAN software and hardware.

A network command will go first to the NetBIOS (Network Basic Input Output System) software, then to the LAN protocol software. The LAN protocol software is unique to the type of LAN. Token Ring software will be different from 10Base5 software, and so forth. The LAN protocol software converts the NetBIOS command to a command that the network Interface card (NIC) can understand. The NIC is a card that plugs into the computer and is the hardware that connects the computer to the LAN. Generally each type of LAN (10Base5 or Token Ring) requires a different type of NIC, but some NICs can support both 10Base2 and 10BaseT. Newer NICs translate between 10BaseT and 100BaseT.

PC without Network Operating Systems

The OS can be DOS or Windows. A command in an application program will call either an OS command, an input device (keyboard) or an output device (printer), or an input/output device (disk drive). If an input, or output, or input/output device is called, the command will be routed to the Basic Input Output System (BIOS) and then to the PC hardware. The BIOS is software written or 'burned' into a read only Memory (ROM) that converts program commands to commands the PC hardware can understand. A ROM stores data even if the power is turned off.

Q. Discuss Peer-to-peer and Client/Server LAN

Peer-to-Peer versus Client/Server

Peer-to peer means there is no dedicated server, yet all workstations within the work group can communicate with each other via the network. No workstation is a server, and all workstations are considered equals or peers. All workstations share resources. A server is a computer dedicated to sending files (serving) to workstations requesting those files; the server allows other computers on the network to use its resources. A client is the computer requesting files from the server.

Q. Explain what a NOS does and Discuss Network monitoring

NOS Functions

A Network Operating System (NOS) transfers files between computers, and between computers and print servers. Often when a user is using a program, such as a word processor, and requests a file, the user is not aware that the file was not residing on his or her machine's hard drive. When a user commands his or her word processor to print a file, the user also is unaware of the file transfer to a print server. The file transfers are 'transparent' to the user.

Network Monitoring

- The NOS monitors who logs in and that the user employs the correct password. The latest NOS versions have elaborate methods of hacker/intruder detection, monitoring, and disabling (shutting out) the hacker.
- NOSs will monitor and log the users for their time on the net. It is possible to monitor a user's e-mail, and the U.S courts have ruled that an employee provides the equipment and connection to the Internet, the company has the right to monitor what is being sent over the net.
- NOSs monitor traffic and are useful to find traffic bottleneck and equipment failures.

Q. What are switches? Explain what you understand briefly

Meaning of Switches

Switches are devices capable of creating temporary connections between two or more devices linked to the switch. In a switched network some of these nodes are connected to the end systems (e.g. computers or telephones) others are used only for routing. Whenever we have multiple devices, we

have the problem of how to connect them to make one –to-one communication possible. We employ Switches to address this problem.

Explain the methods of switching

Methods of Switching

Three methods of switching exist: circuit switching, packet switching, and message switching. The first two are commonly used today. Naturally this divides today's networks into three broad categories: circuit-switched networks, packet-switched networks, and message-switched networks. Packet-switched networks can further be divided into two subcategories; virtual-circuit networks and datagram networks. Networks route the first packet based on the datagram addressing idea, but then create a virtual-circuit network for the rest of the packets coming from the same source and going to the same direction. In message switching, each switch stores the whole message and forwards it to the next switch.

Q. List the three traditional switching methods. What are the most common today?

Three methods of switching exist:

1. Circuit switching
2. Packet switching
3. Message switching.

The first two are commonly used today.

Q. Describe the need for switching and define a switch.

Switching Computers

Switching is done by special purpose computers, designed specifically for switching. The software can easily be replaced and updated. The actual switching is handled by the software, or Stored Program Control (SPC). The "workhorses" of the switching computers are the Electronic Switching System (ESS). The Switching Computers or ESS of the Lucent Technologies are the 4ESS and 5ESS. They can handle up to 1,200,000 calls per hour and 200,000 calls per hour respectively. The 4ESS is used in high demand areas, and the 5ESS is used in lower usage in lower usage areas.

Q. Discuss extensively the structure and component of switches.

Structure of A Switch

We use switches in circuit-switched and packet-switched networks. In this section, we discuss the structures of the switches used in each type of network.

Structure of Circuit Switches: Circuit switching today can use either of two technologies: the space division switch or the time-division switch.

Space-Division Switch: In space-division switching, the paths in the circuit are separated from one another spatially. This technology was originally designed for use in analog networks but is used currently in both analog and digital networks. It has evolved through a long history of many designs.

Crossbar Switch A crossbar switch connects n inputs to m outputs in a grid, using electronic microswitches (transistors) at each cross point. The major limitation of this design is the number of crosspoints required. To connect n inputs to outputs using a crossbar switch requires n x m crosspoints. For example, to connect,, 1000 inputs to 1000 outputs requires a switch with 1,000,000 crosspoints. A crossbar with this number of crosspoints is impractical. Such a switch is also inefficient

because statistics show that, in practice, fewer than 25 percent of the crosspoints are in use are in use at any given time. The rest are idle.

To design a three-stage switch, we follow these steps:

i. We divide the N input lines into groups, each of n lines. For each group, we use one crossbar of size n x k, where k is the number of crossbars in the middle stage. In other words, the first stage has N/n crossbars of n x k crosspoints.

2. We use k crossbars, each of size (N/n) x (N/n) in the middle stage.

3. We use N/n crossbars, each of size k x n at the third stage.

Q. Write short note on the following: Input Ports, Output Port and Routing Processor

i. Input Ports

An input port performs the physical and data link functions of the packet switch. The bits are constructed from the received signal. The packet is decapsulated from the frame. Errors are detected and corrected. The packet is now ready to be routed by the network layer. In addition to a physical layer processor and a data link processor, the input port has buffers (queues) to hold the packet before it is directed to the switching fabric.

ii. Output Port

The output port performs the same function, as the input port, but in the reverse order. First the outgoing packets are queued, then the packet is encapsulated in a frame, and finally the physical layer functions are applied to the frame to create the signal to be sent on the line.

iii. Routing Processor

The routing processor performs the functions of the network layer. The destination address is used to find the address of the next hop and, at the same time, the output port number from which .the, packet is sent-out. This activity is sometimes referred to as table lookup because the routing processor searches the routing table. In the newer packet switches, this function of the routing processor is being moved to the input ports to facilitate and expedite the process.

Q. Write notes on the following switches

i. Multistage Switch

A multistage switch that uses the Clos criteria and a minimum number of crosspoints still requires a huge number of crosspoints. For example, to have a 100,000 input/output switch, we need something close to 200 million crosspoints (instead of l0 billion). This means that if a telephone company needs to provide a switch to connect 100,000 telephones in a city, it needs 200 million crosspoints. The number can be reduced if we accept blocking. Today, telephone companies use time-division switching or a combination of space- and time-division switches, as we will see shortly.

ii. Time-Division Switch

Time-division switching uses time-division multiplexing (TDM) inside a switch. The most popular technology is called the time-slot interchange (TSI). Time-Slot Interchange Imagine that each input line wants to send data to an output line according to the following pattern: 1-3 2 – 4 3 – 1 4 – 2

iii. Banyan Switch

A more realistic approach than the crossbar switch is the banyan switch (named after the banyan tree). A banyan switch is a multistage switch with micro switches at each stage that route the packets based

on the output port represented as a binary string. For n inputs and n outputs, we have log2n stages with nit micro switches at each stage. The first stage routes the packet based on the high-order bit of the binary string. The second stage routes the packet based on the second high-order bit, and so on. Figure 6.9 shows a banyan switch with eight inputs and eight outputs. The number of stages is log2 (8) = 3.

Cryptography

Cryptography, a word with Greek origins, means "secret writing." However, we use the term to refer to the science and art of transforming messages to make them secure and immune to attacks. Network security is mostly achieved through the use of cryptography, a science based on abstract algebra. The original message, before being transformed, is called plaintext. After the message is transformed, it is called cipher text. An encryption algorithm transforms the plaintext into cipher text; a decryption algorithm transforms the cipher text back into plaintext. The sender uses an encryption algorithm, and the receiver uses a decryption algorithm.

Q. Define various terms in cryptography

Definition of Terms

i. Cipher

We refer-to encryption and decryption algorithms as ciphers. The term cipher is also used to refer to different categories of algorithms in cryptography. This is not to say that every sender-receiver pair needs their very own unique cipher for a secure communication. On the contrary, one cipher can serve millions of communicating pairs.

ii. Key

A key is a number (or a set of numbers) that the cipher, as an algorithm, operates on. To encrypt a message, we need an encryption algorithm, an encryption key. and the plaintext. These create the cipher text. To decrypt a message, we need a decryption algorithm, a decryption key, and the cipher text. These reveal the original plaintext.

Alice, Bob, and Eve

In cryptography, it is customary to use three characters in an information exchange scenario; we use Alice, Bob, and Eve. Alice is the person who needs to send secure data. Bob is the recipient of the data. Eve is the person who somehow disturbs the communication between Alice and Bob by intercepting messages to uncover the data or by sending her own disguised messages. These three names represent computers or processes that actually send or receive data. or intercept or change data.

Categories of cryptography

We can divide all the cryptography algorithms (ciphers) into two groups: symmetric key (also called secret-key) cryptography algorithms and asymmetric (also called public-key) cryptography algorithms.

i. Symmetric-Key Cryptography

In symmetric-key cryptography, the same key is used by both parties. The sender uses this key and an encryption algorithm to encrypt data; the receiver uses the same key and the corresponding decryption algorithm to decrypt the data.

ii. Asymmetric-Key Cryptography

In asymmetric or public-key cryptography, there are two keys: a private key and a public key. The private key is kept by the receiver. The public key is announced to the public. In Figure 3.4, imagine

Alice wants to send a message to Bob. Alice uses the public key to encrypt the message. When the message is received by Bob, the private key is used to decrypt the message.

Q. Outline the three types of Keys in Cryptography?

Three Types of Keys

The reader may have noticed that we are dealing with three types of keys in cryptography:

The secret key, the public key, and the private key. The first, the secret key, is the shared key used in symmetric-key cryptography. The second and the third are the public and private keys used in asymmetric key cryptography.

Cipher Block Chaining (CBC)

The cipher block chaining (CBC) mode tries to alleviate some of the problems in ECB by including the previous cipher block in the preparation of the current block. If the current block is i, the previous ciphertext block Ci-1 is included in the encryption of block t‘ In other words, when a block is completely enciphered, the block is sent, but a copy of it is kept in a register (a place where data can be held) to be used in the encryption of the next block. The reader may wonder about the initial block. There is no ciphertext block. 11 before the first block. In this case, a phony block called the initiation vector (IV) is used. Both the sender and receiver agree upon specific predetermined IV. In other words, the IV is used instead of the nonexistent Co. Figure 30.21 shows the CBC mode.

Characteristics of CBC

The following are some characteristics of CBC.

l. Even though the key and the encryption/decryption algorithm are the same, equal blocks in the plaintext do not become equal blocks in the ciphertext. For example, if plaintext blocks 1, 5, and 9 are the same, ciphertext blocks 1, 5, and 9 will not be the same. An adversary will not be able to-guess from the ciphertext that two blocks are the same.

2. Blocks are dependent on each other. Each block is encrypted or decrypted based on a previous block. A problem in encryption or decryption of a block affects other blocks.

3. The error in one block is propagated to the other blocks. If one or more bits are corrupted during the transmission, it affects the bits in the next blocks of the plaintext after decryption.

Cipher Feedback

The cipher feedback (CFB) mode was created for those situations in which we need to send or receive r bits of data, where r is a number different from the underlying block size of the encryption cipher used. The value of r can be 1, 4, 8, or any number of bits. Since all block ciphers work on a block of data at a time, the problem is how to encrypt just r bits. The solution is to let the cipher encrypt a block of bits and use only the first r bits as a new key (stream key) to encrypt the r bits of user data. Figure 30.22 shows the configuration.

The following are some characteristics of the CFB mode:

1. If we change the IV from one encryption to another using the same plaintext, the ciphertext is different.

2. The ciphertext Ci depends on both Pi and the preceding ciphertext block.

3. Error in one or more ciphertext block affects the next ciphertext blocks.

Output Feedback

The output feedback (OFB) mode is very similar to the. CFB mode with one difference. Each bit in the ciphertext is independent of the previous bit or bits. This avoids error propagation. If an error occurs in transmission, it does not affect the future bits. Note that, as in CFB, both the sender and the receiver use the encryption algorithm. Note also that in OFB, block ciphers such as DES or AES can only be used to create the key stream. The feedback for creating the next bit stream comes from the previous bits of the key stream instead of the ciphertext. The ciphertext does not take part in creating the key stream. Figure 30.23 shows the OFB mode.

The following are some of the characteristics of the OFB mode

1. If we change the IV from one encryption to another using the same plaintext, tile, ciphertext will be different.

2. The ciphertext Ci depends on the plaintext Pi.

3. Errors in one or more bits of the ciphertext do not affect future ciphertext blocks.

Selecting Keys

Bob use the following steps to select the private and public keys:

1. Bob chooses two very large prime numbers p and q. Remember that a prime number is one that can be divided evenly only by 1 and itself.

2. Bob multiplies the above two primes to find n, the modulus for encryption and decryption. In other words, $n = p \times q$.

3. Bob chooses a random integer e. He then calculates d so that $d \times e = 1 \bmod \varphi$.

4. Bob announces e and n to the public; he keeps φ and d secret

Q. Discuss the five services provided by Network security.

Security Services

Four of these services are related to the message exchanged using the network: message confidentiality, integrity, authentication, and nonrepudiation. The fifth services provides entity authentication on identification.

1. Message Confidentiality

Message confidentiality or privacy means that the sender and the receiver expect confidentiality. The transmitted message must make sense to only the intended receiver. To all others, the message must be garbage. When a customer communicates with her bank, she expects that the communication is totally confidential.

2. Message Integrity

Message Integrity means that the data must arrive at the receiver exactly as they were sent. There must be no changes during the transmission, neither accidentally or maliciously. For instance it will be disastrous if a request for transferring N 300,000 is changed to N 3,000,000.

3. Message Authentication

Message authentication is a service beyond message integrity. In message authentication the receiver is to be sure of the sender's identity and that an imposter has not sent the message.

4. Message Non repudiation

Message nonrepudiation means that a sender must not be able to deny sending a message that he or she did send. The burden of proof falls on the receiver. For example when a customer sends a message to transfer money from one account to another, the bank must have proof that the customer actually requested the this transaction.

5. Entity Authentication

In entity authentication the entity or user is verified prior to access to the system resources. For example, a student who needs to access her university resources needs to be authenticated during the logging process. This protects the interest of the university and the student.