Module 1

Introduction to Computer Network

INTRODUCTION TO COMPUTER NETWORK

Ques 1) What is computer network? What are the main components of computer network? List them.

Or

Give the introduction of computer network.

Ans: Computer Network

"A computer network is a group of computers linked to each other that enables the computer to communicate with another computer and share their resources, data, and applications."

Network allows the computers to exchange the data and information via data connection and these data travel in the form of **packets** through various nodes in the network.

Computer network can be considered as information highways for data.

Components of Data Communication

The fundamental components of the communication system are given below:

1) Transmitter
2) Transmission Medium
3) Receivers
4) Hardware
5) Communication Network
6) Communication Software
7) Data Communication Providers
8) Communication Protocols

Ques 2) What are the advantages and disadvantages of networks?

Or

Write any three disadvantages of using computer network.

Ans: Advantages of Networks

1) **Resource Sharing:** A computer network provides the facility of resource sharing. Resource sharing deals with the sharing of resources (such as printer etc.) among various nodes or client of a computer network.
2) **High Reliability:** It's a property of computer network where network provides substitute source of supply. **For example,** a client can duplicate the files on two or more than two node in a network, so if one node is fail or unavailable then client get the file from another computer.
3) **Communication Medium:** Very powerful communication medium can be provided by a computer network between separated clients giving the virtual absence of geographical boundaries.
4) **Increased Productivity:** On computer network two or more process handled at the same time. **For example,** one client can handle account receivable and another process the profit and loss statements.

Disadvantages of Networks

1) **Crashes:** The major problem in a server based network is that when server is crashes then no one (client) can access the network resources. Clients lost the all benefits available in that network. So for the security reason backups are always taken because crash may result in the loss of days and even in month of time and data.
2) **Data Security:** If proper precautions and security will not be taken then it is possible that an unauthorized employ can access classified information. So, proper implementation of security is necessary.
3) **Privacy:** Privacy is a big issue in network. **For example,** one can (like your boss) read private mails by changing some privileges setting in the network.

Ques 3) What are the uses of network?

Or

What are the main applications of network?

Or

Describe any three application of computer network.

(2021[03])

Ans: Uses of Networks/Applications of Network

Following are the few common applications of computer networks:

1) **Business Applications:** There are sufficient numbers of computer to several companies. **For example,** to monitor the production, for keep trac**(2021[04])**tories and to do the payroll, company may have separate computers. At the beginning every computer may have their functioning in separate manner from the others, but management may have decided to connect them at some point in order to extract and correlate information about the whole company.
2) **Home Applications:** In the home, the network is mainly used as Internet. Following are the various more popular uses of the Internet for home users:
   i) Access to Remote Information
   ii) Person-to-Person Communication
   iii) Interactive Entertainment

3) **Mobile Users:** People often want to send and receive their telephone calls, faxes, and electronic mail by using their portable electronic devices. They surf the web so that they can access remote files and log onto remote machines and they want to do it from anywhere.

NETWORK HARDWARE

Ques 4) What are the different types of networks? Explain them.

Or

What is LAN, MAN and WAN?

Or

How are computer networks classified on the basis of physical size. (2018[03])

Or

Explain WAN? (2019[01])

Ans: Types of Network/ Classification of Computer Networks on the Basis of Physical Size

1) **Local Area Network (LAN):** Local Area Network (LAN) is a group of computers that provides reliable high speed communication channels for associated information processing devices in a small geographical area such as campus, office building, etc.

Figure 1.1: LAN Architecture

In a LAN, computers and peripherals are interconnected through a common medium in order that users can access the host computers, application files, etc.

If there are two LANs then one can access both the LANs using a dedicated device known as **gateway** or using a computer which is authorised and connected with both the networks.

LANs are basically used in college, university, industry & business organisations, science & engineering, etc. With the development of LAN users may achieve a paperless office. IEEE (Institute of Electrical and Electronics Engineers) developed specification for LANs. LANs provide a bandwidth of 1 Mbps to 100 Mbps or even more. Organisations can also extend the area of LAN by using some network devices such as bridges, routers, etc.

2) **Metrop** larger than LAN and can cover a city and its surrounding areas. Generally, MANs can be created by interconnecting two LANs. Geographical cover area of MAN is larger than LAN but smaller than Wide Area Network (WAN).

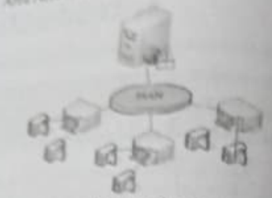


Figure 1.2: Metropolitan Area Network

These networks deliver fast and efficient communication by using a high-speed carrier, e.g., fibre optic cables.

Area of MAN lies between the LAN and MAN and can cover approximately 50 km of diameter or sometimes entire city.

MAN is owned either by a group of people or by single network provider. This service provider gives the network service to many users. **Figure 1.2** shows a Metropolitan Area Network.

3) **Wide Area Network (WAN):** WAN connects devices of a larger geographical area (area that is not served by the LAN and MAN) and uses common carriers like satellite systems, telephone line, etc., to facilitate the transmission. It works at the physical layer, the data link layer and the network layer of Open System Interconnection (OSI) model. **Figure 1.3** shows a WAN.

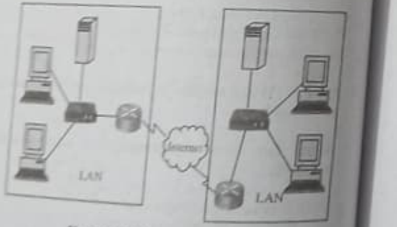


Figure 1.3: Wide Area Network (WAN)

The most useful example of WAN is Internet.

Ques 5) What is difference between LAN, MAN and WAN?

Ans: Difference between LAN, MAN and WAN

Table 1.1 shows the difference between LAN, MAN and WAN.

Table 1.1: Difference between LAN, MAN and WAN

Basis	LAN	MAN	WAN
Coverage	Diameter of not more than a few kilometres.	Diameter covers a town or a city.	Covers entire countries.
Data Rate	A total data rate of at least 10 to 100Mbps.	Total data rate is variable.	Data rate more than 1 Mbps (Megabits per second).
Ownership	Complete ownership by a single organisation	Complete ownership is collectively held by few (3-4) organisations.	Owned by multiple organisation.
Error Rate in Data Transmission	Very low error rates.	Low error rate.	Comparatively higher error rates.
Topology used	Symmetrical topology.	Distributed Queue Dual Bus.	Irregular topologies.

Ques 6) What are point to point and broadcast networks? (2019[03])

Or

How are computer networks classified on the basis of transmission technology.

Ans: Classification of Network by Transmission Technology

Basically there are two types of transmission technology:

1) **Broadcast Networks:** The transmission of data from one node to another node is called broadcasting. It is a type of transmissión technique.

Broadcasting systems typically use a code in the address field to allow all destinations on the broadcast network to be addressed by a packet.

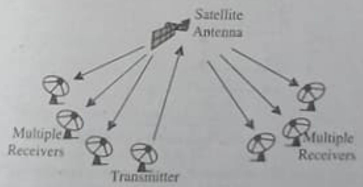


Figure 1.4: Broadcast Network

A single communication channel that is shared by all other nodes is called a broadcast network. The code is received and processed by every machine on the network when a packet with this code is transmitted.

2) **Point-to-Point Networks:** Where a single communication channel is not shared by all nodes then this is a peer-to-peer or point-to-point transmission in the network. But it involves sharing of the communication channel (as occurs in the ring topology) between only two adjacent nodes. When a packet (data) is sent between two nodes then the packet is transferred from the source node to its nearby node.

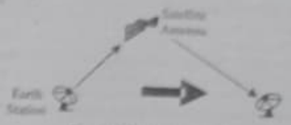


Figure 1.5: Point to Point Network

The address part is checked after receiving the packet and it is regenerated if the packet is not intended for that node. The routing algorithms play an important role in point to point communication when packet is passes through adjoining node. Until packet is not reaches the destination, it is passed on like this. This type of transmission is done over the Metropolitan Area Network (MAN) and Wide Area Network (WAN).

Ques 7) What is internetwork? Also define communication subnet in detail.

Or

Explain communication subnet? (2019[1])

Ans: Internetworks

An internetwork is defined as a collection of individual networks, attached by intermediate networking devices and functions as a single large network. **Internetworking** refers to the industry, products, and method that fulfil the challenge of creating and administering internetworks.

When one connect more than two or more networks using intermediary devices then this process is known as Internetworking. Using the common data communication and the Internet Routing Protocol (IRP) internetworking confirms the communication among networks operated by different entities.

Communication Subnet

Today's networks are not constrained by the inability of LANs to cover distance and manage mobility. WANs provide long-distance transmission of data, voice, image and video information over large geographical areas that may include a country, a continent or even the entire world.

It consists of a collection of machines, called hosts, which run user (application) programs. The hosts are linked by a communication subnet, which performs the task of carrying messages from host to host.

The WAN combines host and collection of machines. User program is installed on the host and machines. All the host are connected by each other through communication subnet. Subnet carries messages from host to host. Communication subnet is also called as **communication subnetwork** or the carrier portion of the system.

NETWORK SOFTWARE

Ques 8) What is protocol? What are the elements of protocols?

Or

Define the terms protocol. (2018[01])

Ans: Protocols

In Computer Network, a protocol is a set of rules and standards followed by network devices for proper communication among them. Some **examples** of protocols are Transmission Control Protocol, Internet Protocol, File Transfer Protocol etc.

Elements of a Protocol

The main elements of a protocol are as follows:

1) **Syntax:** Syntax means the format or structure of the data fields. It denotes the order in which data are arranged.

2) **Semantics:** It denotes the meaning of every section of data bits. It specifies how specified data pattern is to be interpreted; and what action is to be performed on interpretation?

3) **Timing:** Timing is used to specify two characteristics:
   i) When data should be transferred.
   ii) How fast they can be transferred.

4) **Semantics:** It denotes the meaning of every section of data bits. It specifies how specified data pattern is to be interpreted; and what action is to be performed on interpretation?

5) **Timing:** Timing is used to specify two characteristics:
   i) When data should be transferred.
   ii) How fast they can be transferred.

Ques 9) Describe protocol hierarchy.

Ans: Protocol Hierarchy

For the help of protocol designers to understand the patterns of communication problem and plan an entire protocol suite, various tools have been developed.

The **layering model** is the most important tools which provide a simple explanation of the relationships among the complex hardware and protocol components of a network.

The objective of every layer is to provide services to its higher layers. In one machine, the layer n carries on a conversation with layer n on another machine. The rules and conventions used for conversation are collectively known as "protocol".

The protocol is an agreement between the communication networks for how to precede the communication. **Figure 1.6** shows that a five-layer network:

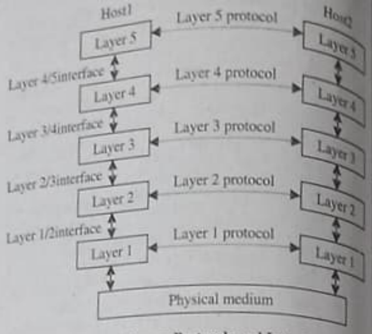


Figure 1.6: Layers Protocols and Interfaces

Ques 10) Explain the layered architecture of computer network.

Or

Write the Working of Layered Architecture.

Ans: Layered Architecture of Computer Network

The division of the organisation into offices and every office functions in hierarchical levels and interaction procedures define the overall organisation architecture.

By using a sub network, a computer network is also partitioned into end systems and communication procedure is divided into hierarchical functional layers as shown in **figure 1.7.**

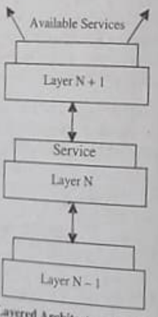


Figure 1.7: Layered Architecture of a Computer Network

Every layer has a distinct identity and a specific set of functions assigned to it, just like in an office. Every layer has an active element consists of hardware or software and it carries out the functions of layer. It is known as **layer entity**.

The reference model is a conceptual blueprint of method of the communication that takes place. It addresses all the methods required for effective communication and divides them into layers. It is called as **layered architecture** if a communication system is designed in this manner.

Working of Layered Architecture

1) The layered architecture simplifies the architecture of complex system.
2) To provide a service to layer N + 1, layer N relies on service from layer N – 1
3) The services offered are separated by interfaces.
4) The service needed from a lower layer is independent of its implementation:
   i) Information hiding.
   ii) Layer N change does not affect other layers.
   iii) Same as object oriented methodology.

Ques 11) What are the reasons for using Layered Architecture in Computer Networks? (2018[01])

Ans: Reasons of Using Layered Architecture in Computer Networks

1) To make the design process easy by breaking unmanageable tasks into several smaller and manageable tasks (by divide-and-conquer approach).
2) Modularity and clear interfaces, so as to provide comparability between the different providers' components.
3) Ensure independence of layers, so that implementation of each layer can be changed or modified without affecting other layers.
4) Each layer can be analysed and tested independently of all other layers.

Ques 12) Discuss about the design issues for the layers.

Or

List the design issues of layered network software. (2019[03])

Or

List out the key design issues that occur in Computer Networks. (2018[04])

Ans: Design Issues of the Layers

Following are the various design issues of the layers:

1) **Addressing:** Every layer requires a mechanism for the source and destination machine. There are two types of addresses:
   i) Destination Address
   ii) Source Address.

2) **Mode of Communication:** The mode of transmission must be taken into consideration for designing the layer. The protocol should be used for congestion control or media access under mode of transmission.

3) **Error Control:** Two types of error control methods are as follows:
   i) Error detecting code.
   ii) Error correcting code.

4) **Sequencing:** By implementing sequence number in their frames, the order of the Packets/Frames must be ensured. Sequence number is required for error control and detection.

5) **Flow Control:** At a slow transmission rate, it considers how to keep fast senders from swapping with a data agreement.

6) **Packet Size:** The size of a standard packet has to be specified to make the transmission compatible. Each strategy has its own standard (frame size) and is strictly followed.

7) **Multiplexing:** There is use of Multiplexing in th physical layer and it is needed when a single media o wire is used by more users.

Ques 13) Write short note on interfaces and services.

Or

What are the different types of services?

Or

Define the term interface. (2018[01

Ans: Interfaces and Services

The process offers a common technique for communicat between layers. The standard terminologies are used layered network to request services.

Figure 1.8 shows three layers (N+1), N and (N-1 which the communication process is taken place for communication.

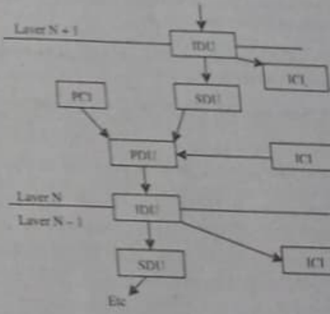


Figure 1.8: Communication between Layers

Following components are involved and their f as follows:

1) **SDU (Service Data Unit):** Transfer user da (N + 1) to layer N and (N – 1).
2) **PCI (Protocol Control Information):** It exchange information by peer entities at dif on the network.
3) **PDU (Protocol Data Unit):** Combination and PCI.
4) **ICI (Interface Control Information):** temporary parameter between N and N – service function.
5) **IDU (Interface Data Unit):** The tot information transferred across the layer **Figure 1.9** illustrates the communication b sites.

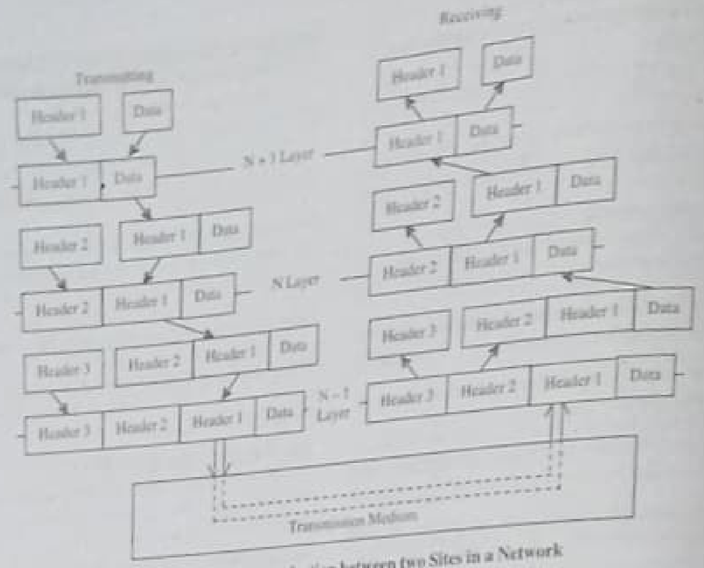


Figure 1.9: Communication between two Sites in a Network

Ques 14) What are Connection Oriented and Connectionless Services?

Or

Give a difference between Connection-Oriented Service and Connectionless Service.

Ans: Connection Oriented and Connectionless Services

There are two types of services:

1) **Connection-Oriented Services:** With known and valid input parameters, the service:
   i) Establishes the connection.
   ii) Allows one to utilize the connection.
   iii) Tears down the connection when work is done using it.

   This method is different from a connectionless service as all of communications are taking place on the same transmission channel in a connection-oriented system.

2) **Connectionless Services:** The process of sending letters through the postal system is a good analogy for a connectionless service. Every transmission (the "letter") contains the full address of the destination and is processed with independent of related messages. The service only ensures that message reaches to its host within certain time parameters specified.

Difference between Connection-Oriented Service and Connectionless Service

Connection-Oriented Service	Connectionless Service
This is needed for service authentication	This does not required any authentication
This protocol makes a connection and checks whether message is received or not and sends again if an error occurs.	This service does not give the delivery guarantee.
It is more reliable.	It is less reliable.
This interface is stream based.	This is message based.

Ques 15) What are the service primitives?

Or

What are the OSI service primitives for connection oriented service? (2018[04])

Ans: OSI Service Primitive

A service is formally specified by a set of primitives (operations) available to a user process to access the service. These primitives tell the service to perform some action or report on an action taken by a peer entity. If the protocol stack is located in the operating system, as it often is, the primitives are normally system calls. These calls cause a trap to kernel mode, which then turns control of the machine over the operating system to send the necessary packets.

The set of primitives available depends on the nature of the service being provided. The primitives for connection-oriented service are different from those of connectionless service. Five service primitive are shown in table below:

Table 1.2: Five Service Primitives for Implementing a Simple Connection Oriented Service

Primitive	Meaning
LISTEN	Block waiting for an incoming connection
CONNECT	Establish a connection with a waiting peer
RECEIVE	Block waiting for an incoming message
SEND	Send a message to the peer
DISCONNECT	Terminate a connection

Ques 16) Distinguish between interface, protocol and layer in network software. (2019[03])

Ans: Difference between Interface, Protocol and Layer

Table 1.3 shows the difference between Interface, Protocol and Layer:

Table 1.3: Difference between Interface, Protocol and Layer

Interface	Protocol	Layer
Interface is a software or hardware interface between two pieces of equipment or protocol layers in a computer network.	A network protocol is a set of rules and standards which must be followed by network devices for proper communication among them.	It divides the network communication process into smaller and simpler components, thus aiding component development, design, and troubleshooting.
For example, link interface, bus interface etc.	**For example,** Transmission Control Protocol, Internet Protocol, File Transfer Protocol etc.	For example, the seven layers of TCP/IP reference models are: i) Application Layer ii) Transport Layer iii) Internet Layer iv) Network Interface Layer
Interface divides the two segments and their working.	Protocol defines the format of data i.e., to be exchanged.	It provides modularity and clear interfaces.

REFERENCE MODELS

Ques 17) What do you understand by Reference Model?

Or

What are the different types of Network Reference Models? List them.

Ans: Reference Model

A network reference model is a conceptual blueprint of how communication should occur. The functions of communication software in a generalized and structured way are clearly defined by network reference model and help to carry out the network activities. The reference model identifies the functions involved in inter-computer communication for efficient communication and divides them into logical groups called **layers**, in which each layer performs a particular function. This type of communication system is known as **layered architecture**.

Need of Network Reference Model

There are various advantages of network reference mode. Some of the needs of network reference model are as follows:

1) This is helpful in various types of network software and hardware to communicate with each other.
2) This specifies the standards for building network components and permits the multiple-vendor development.

Types of Network Reference Models

There are two types of network models:

1) ISO- OSI Model
2) TCP/IP Model

Ques 18) Describe the ISO/OSI layered architecture with the help of a neat diagram. (2018[05])

Or

With neat diagram, explain OSI Reference Model. (2019[06])

Or

What are the functions of different layers of OSI reference model?

Or

Write the functions of presentation and session layer of OSI reference model. (2021[03])

Ans: ISO-OSI Reference Model

Open Systems Interconnection (OSI) is a reference model which defines the way in which messages are to be transmitted between any two points in the network.

Figure 1.10 illustrates the OSI reference model:

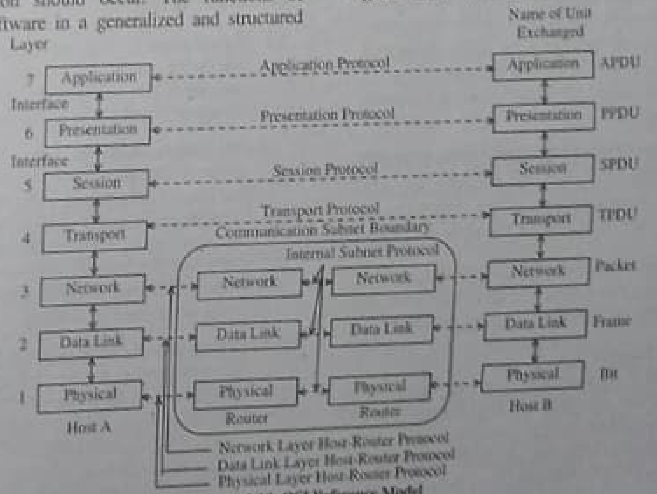


Figure 1.10: OSI Reference Model

where,

APDU – Application Protocol Data Unit
PPDU – Presentation Protocol Data Unit
SPDU – Session Protocol Data Unit
TPDU – Transport Protocol Data Unit

Layers of OSI Model and Their Functions

The different layers of the OSI reference model are:

1) **Application Layer:** Users and application processes access network services through the application layer. Mail, FTP, Telnet, DNS, NIS and NFS are all **examples** of network applications.

Functions of Application Layer

i) **Authentication:** It authenticates either the sender or receiver of the message or both.

ii) **File Access, Transfer and Management:** It provides access to a remote user on another host to files on a server.

iii) **Directory Services:** It enables access to global information and database sources.

2) **Presentation Layer:** The presentation layer works as a data translator for a network which is part of an operating system.

Functions of Presentation Layer

Couple of functions of presentation layer are as follows:

i) **Data Compression:** This refers to a process of encoding data using lower number of bits which increases the efficiency of data transmission.

ii) **Encryption:** This provides security by way of algorithms for coding, passwords and log-in-codes.

3) **Session Layer:** The function of the session layer is to facilitate communication among the processes running in various modules over a network.

Functions of Session Layer

i) **Session Management:** Checkpoints are inserted into the sessions to divide them into sub-sessions.

ii) **Synchronisation:** The order, in which the dialog units are to be passed to the transport layer, is selected. Confirmation is also obtained from the receiver machine.

iii) **Dialog Control:** It controls who will send the data and when.

iv) **Closing the Session:** It ensures the completion of data transfer before closing of the session.

4) **Transport Layer:** Function of the transport layer is to ensure that the messages are transmitted in the intended order and no duplication or loss occurs.

Functions of Transport Layer

i) **Service-Point Addressing:** In the transport layer header has the port address also known as the service-point address. The transport layer is able to send the packet to the intended process with the help of the port addresses.

ii) **End-to-End Message Delivery:** It guarantees that the complete message has been received by the destination.

iii) **Connection Control:** Whether the packets will be sent along the same path or not is decided.

5) **Network Layer:** The task of this layer is to determine the physical path to be followed by the data based on various factors such as service priority and conditions of the network. It forwards and routes the packets.

Functions of Network Layer

i) **Source-to-Destination Delivery:** The packet is transferred from source to destination.

ii) **Logical Addressing:** The source and destination address is appended to the header.

iii) **Routing:** For the packet to flow, the optimal path out of a number of paths is chosen.

iv) **Address Transformation:** The logical address is interpreted.

v) **Multiplexing:** A single physical line is used to transfer data between several devices simultaneously.

6) **Data-Link Layer:** The data-link layer ensures that the data frames are transferred without any error. The layer offers synchronisation to the physical layer. The data format to be used by the network is defined by the data link layer.

Data Link Layer: Sub-Layers

There are two sub-layers that comprise the IEEE Ethernet Data Link layer:

i) Logical Link Control (LLC) 802.2
ii) Media Access Control (MAC) 802.3

Functions of Data-Link Layer

i) **Framing:** The prime concern is to determine the start and end of the successive packets. This problem is solved by encapsulating the packets in a frame. This is done by the DLC by adding its header and trailer.

ii) **Arbitration:** The process of arbitration determines how the access to a single data channel will be given when more than one host is trying to access it simultaneously.

iii) **Physical Addressing:** There is difference between network addressing and physical addressing. With the help of the network addresses in a network it is possible to identify the devices or nodes in a network uniquely. This allows the packets to be switched or routed over the network. Media Access Control (MAC) address is the primary form of physical addressing.

iv) **Error Detection:** In order to detect the occurrence of error during bit transfer across the wire, error detection is carried out. CRC (Cyclic Redundancy Check) is a value that is calculated by the Data Link layer. This value is placed in the trailer of the Data Link layer. Before sending the message to the Physical layer, this trailer is appended.

v) **Encapsulation:** DLL has the ability to recognise the data that has been encapsulated. With the help of encapsulation, it is possible to implement modular communication. Using this feature, the functions that are logically different are **abstracted** from the structures lying below. This is done by information hiding between the objects lying at higher levels.

7) **Physical Layer:** The prime task of physical layer is the packaging and transmission of the data via physical layer. The bit streams are propagated over the network in the form of mechanical and electrical signals.

Functions of Physical Layer

i) **Line Configuration:** The physical connection between two or more devices is defined.

ii) **Data Transmission:** The transmission mode between two devices is defined.

iii) **Topology:** Arrangement of the devices in a network is defined.

iv) **Signals:** The signal type used for information transmission is defined.

Ques 19) What is TCI/IP reference model?

Or

Write the Function of TCP/IP-Layers.

Or

Explain TCP/IP reference model with the help of a diagram. (2021[05])

Ans: TCP/IP Reference Model

Communication among computers became a challenge with the increase in the number of computers connected to ARPANET. As the hardware and software was vendor specific in nature, common standards were necessary to carry out the communication.

The computers required common protocols to carry out the communication and as a result, TCP and IP were designed. In order to address the increasing number of requirements, a number of protocols were designed. The new reference model known as **TCP/IP reference model** was also created.

Figure 1.11 illustrates the four layers of TCP/IP model. They are Application, Transport, Internet, and Network Interface.

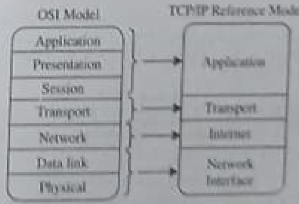


Figure 1.11: TCP/IP Reference Model is a Standard Reference Model for Communication in the Internet

The top three layers comprise of all the protocols belonging to the TCP/IP protocol suite.

Functionality of TCP/IP-Layers

1) **Network Access Layer:** The network layer carries out the task of transferring data between devices that belong to the same network and between network and a host.

2) **Internet Layer:** The task of the internet layer is to send source packets between different networks in the internetwork.

3) **Transport Layer:** The transport layer ensures flow control and reliability of the data being transmitted over the network. Apart from this, it also performs error correction.

4) **Application Layer:** The main functionalities provided by this layer are management of high-level protocols, representation problems, data encoding and control of the dialog.

Ques 20) What is difference between OSI and TCP/IP reference model?

Or

Compare TCP/IP Reference model and OSI Reference model. (2019[03])

Ans: Comparison between OSI and TCP/IP Reference Models

Table 1.4 shows the differences in both models.

Table 1.4: OSI versus TCP

Basis	OSI	TCP
No. of Layers	7 Layers	4 Layers
Implementation	The model was defined before implementation of any protocol was available.	When protocols were implemented after that the model was defined.
Model Concepts	It defines service, interface and protocol very clearly. It is protocol independent.	It does not clearly distinguish between service, interface and protocol. It is protocol dependent.
Delivery of Packets	Its transport layer gives guarantee of reliable delivery of a packet.	Its transport layer does not always guarantee delivery of packet.
Internet working	It does not support internet working.	It supports internet working.

PHYSICAL LAYER

Ques 21) What is physical layer? What are the functions of physical layer?

Ans: Physical Layer

Physical layer defines the cable or physical medium itself, e.g., thinnet, thicknet, Unshielded Twisted Pairs (UTP). All media are functionally equivalent. The main difference is in convenience and cost of installation and maintenance. Converters from one media to another operate at this level. The physical layer is responsible for packaging and transmitting data on the physical media. This layer conveys the bit streams through the network at the electrical and mechanical level.

Functions of Physical Layer

The major functions of physical layer are given below:

1) **Line Configuration:** Defines the way in which two or more devices can be connected physically.
2) **Data Transmission:** Defines the transmission mode between the two devices on the network.
3) **Topology:** Determines the way in which the network devices are arranged.
4) **Bit to Signal Transmission:** Determines the type of signal that is used for transmitting information.

Ques 22) Discuss about the modes of communication with suitable figure.

Or

Define simplex, half-duplex, and fill duplex transmission modes. Give one example for each.

Ans: Mode of Communication

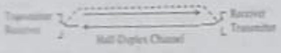
The transmission mode provides the direction to any communication channel. The various modes of data transmission are:

1) **Simplex Communication:** In a simplex channel, data movement is always one way, i.e., it cannot send back error or control signals to the transmit end.

Transmitter
Receiver
Simplex
Channel

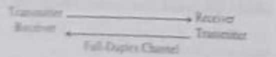
For example, televisions and radios use the simplex channel.

2) **Half-Duplex Communication:** A single physical channel where the direction may be reversed is referred to as the **half-duplex channel**. This implies that messages flow in from either direction but never at the same time.



For example, in a telephone conversation, one party listens when the other party speaks and vice versa. If both parties speak simultaneously, then it results in garbled sound which is difficult to understand.

3) **Full-Duplex Communication:** This allows two way communications at the same time.



For example, if a consumer uses such a cable connection which also provides phone and internet facility, then all three can be used simultaneously.

Ques 23) What are physical topologies?

Or

Define the basic LAN topologies.

Ans: Physical Topologies

Network topology is the pattern used to arrange (physically or logically) the nodes or stations of a network.

Basic LAN Topologies

Basically there are five types of network topologies:

1) **Bus Topology:** It is the simplest physical network. In this topology all the computers including servers are connected by a single cable with the help of interface connectors. The cable is known as **bus** and acts as backbone of the network which joins every computer and peripheral in the network (**figure 1.12**):

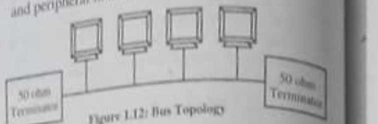


Figure 1.12: Bus Topology

2) **Ring Topology:** In a ring topology all the computers (nodes) are connected in a closed loop. This topology works on the token based system and token travels in the loop. If token is free, then the node can capture the token and attach the data and destination address to the token, and then leaves the token.

When token reaches at the destination node the data is removed by the destination node and token is free to carry the next data. If another node wants to send the data, it can capture the free token. In this topology each node or computer works as a **repeater**.

The main drawback of ring topology is that if one node fails, then the complete network will go down. The figure 1.13 shows a ring topology

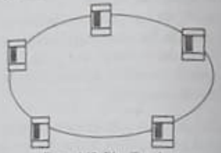


Figure 1.13: Ring Topology

3) **Star Topology:** This is a most popular topology to create a network. In this topology nodes are attached with a centrally located device known as **hub** with **UTP** (Unshielded Twisted-Pair) wire. In this topology data are transferred from one node to another node via hub.

In star topology each computer (node) has a distinct connection to the hub, so it is easy to maintain and troubleshoot it. **Figure 1.14** shows the example of star topology.

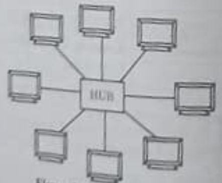


Figure 1.14: Star Topology

4) **Mesh Topology:** In a mesh topology (**figure 1.15**) all the computers are associated with each other via various redundant connections. So there are many paths for data delivery from one computer to another computer.

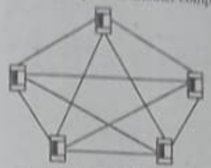


Figure 1.15: Mesh Topology

Mesh topology provides two types of connection management:

i) **Full Mesh Topology:** In this topology, each computer or device is connected to all other computers or devices in a network.

ii) **Partial Mesh Topology:** In this topology, not all but only certain computers or devices are connected to those computers or devices with which they communicate frequently. While, other remaining computers (nodes) are connected to all computers (nodes).

5) **Tree Topology:** In a tree topology (**figure 1.16**) all the computers are connected with each other in hierarchical fashion. The top most node of the network is known as **root node.** Except the root node, all other nodes have exactly single parent node, while all the nodes in the tree are descendants of the root node. So, only one path exists for data transmission from one node to other node in the tree topology.

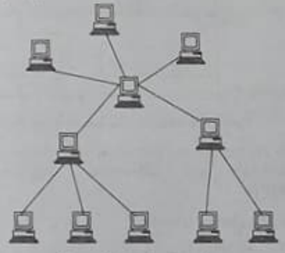


Figure 1.16: Tree Topology

SIGNAL ENCODING

Ques 24) What is signal encoding and decoding? What is the purpose of encoding?

Ans: Encoding and Decoding

Encoding is the process of putting a sequence of characters (letters, numbers, punctuation, and certain symbols) into a specialized format for efficient transmission or storage.

Decoding

Decoding is the opposite process – the conversion of an encoded format back into the original sequence of characters. Encoding and decoding are used in data communications, networking, and storage. The term is especially applicable to radio (wireless) communications systems.

Purpose of Encoding

1) Encoding is done to reduce the number of bit to be transmitted and save bandwidth.
2) Error correction encoding adds more information to the data stream to allow for this reconstruction; thus, adding error correction encoding always increases the length of the data.
3) Encoding is used to make the form of the spectrum of a digital signal suitable for a certain communication media.
4) Encoding is used to help to synchronize the receiver.
5) Encoding can be used to increase the data rate.

Ques 25) What are the different encoding techniques? Explain.

Or

Explain the Manchester and differential Manchester encoding.

Ans: Encoding Techniques

1) **Polar Schemes:** In polar schemes, the voltages are on the both sides of the time axis. **For example,** the voltage level for 0 can be positive and the voltage level for 1 can be negative.

Types of Polar Encoding

i) **Non Return to Zero (NRZ):** NRZ codes share the property that voltage level is constant during a bit interval. High level voltage = bit 1 and Low level voltage = bit 0. A problem arises when there is a long sequence of 0s or 1s and the voltage level is maintained at the same value for a long time. This creates a problem on the receiving end because now, the clock synchronization is lost due to lack of any transitions and hence, it is difficult to determine the exact number of 0s or 1s in this sequence.

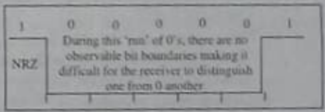

1
0
0
0
0
0
1
NRZ
During this 'run' of 0's, there are no observable bit boundaries making it difficult for the receiver to distinguish one from 0 another

Figure 1.17: NRZ Encoding

The two variations are as follows:

a) **NRZ-Level:** In NRZ-L encoding, the polarity of the signal changes only when the incoming signal changes from a 1 to a 0 or from a 0 to a 1. NRZ-L method looks just like the NRZ method, except for the first input one data bit. This is because NRZ does not consider the first data bit to be a polarity change, where NRZ-L does.

b) **NRZ-Inverted:** Transition at the beginning of bit interval = bit 1 and No Transition at beginning of bit interval = bit 0 or vice versa. This technique is known as differential encoding.

ii) **Return to Zero (RZ):** The main problem with NRZ encoding occurs when the sender and receiver clocks are not synchronized. The receiver does not know when one bit has ended and the next bit is starting. One solution is the return-to-zero (RZ) scheme, which uses three values: positive, negative, and zero. In RZ, the signal changes not between bits but during the bit. In **figure 1.18** we see that the signal goes to 0 in the middle of each bit. It remains there until the beginning of the next bit.

The main **disadvantage** of RZ encoding is that it requires two signal changes to encode a bit and therefore occupies greater bandwidth.

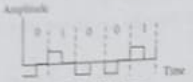


Figure 1.18 Polar RZ scheme

iii) **Bi-Phase Encoding:** Biphase encoding is a variation on polar encoding and is an effective answer to synchronisation problems. Biphase encoding works by changing the signal in the middle of the bit interval, however, the signal does not then return to zero it continues to the opposite pole. This mid-interval change is perfect for synchronisation purposes.

It has following **characteristics**:

a) Modulation rate twice that of NRZ and bandwidth correspondingly greater. Modulation is the rate at which signal level is changed.

b) Because there is predictable transition during each bit time, the receiver can synchronize on that transition i.e. clock is extracted from the signal itself.

c) Since there can be transition at the beginning as well as in the middle of the bit interval the clock operates at twice the data transfer rate.

Types of Bi-Phase Encoding

a) **Biphase-Manchester Encoding:** This encoding scheme is a combination of RZ and NRZ-L. Bit time is divided into two halves. It transits in the middle of the bit and changes phase when a different bit is encountered.

b) **Differential-Manchester Encoding:** Always a transition in middle of interval. No transition at beginning of interval=1 and Transition at beginning of interval = 0

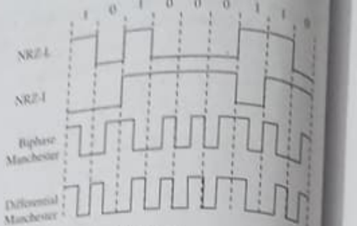


Figure 1.19:

2) **Bipolar Schemes:** In bipolar encoding (sometimes called **multilevel binary**), there are three voltage levels: positive, negative, and zero. The voltage level for one data element is at zero, while the voltage level for the other element alternates between positive and negative.

Two variations of bipolar encoding:

1) **Alternate Mark Inversion (AMI):** In this code, a binary 0 is encoded as zero volts, as in unipolar encoding, whereas a binary 1 is encoded alternately as a positive voltage or a negative voltage.

2) **Pseudoternary:** Pseudoternary has the same behavior as Bipolar-AMI except it reverses signaling:

i) 1 = no signal (0 voltage)

ii) 0 = alternating +V and – V

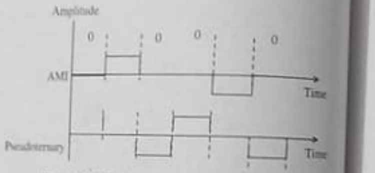
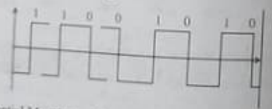


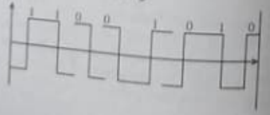
Figure 1.20: Bipolar Schemes: AMI and Pseudoternary

Ques 26) Encode the following binary data stream into Manchester and differential Manchester codes 11001010.

Ans: Manchester Encoding:



Differential Manchester Encoding:



Ques 27) Draw the waveform for 1100111O in each of the following encoding method:

i) **NRZ-I**

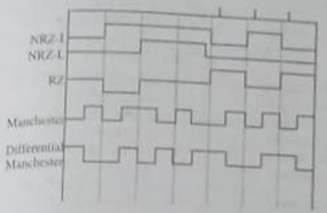
ii) **NRZ-L**

iii) **RZ**

iv) **Manchester**

v) **Differential Manchester.**

Ans: The waveforms one drawn in the figure, the illustration is given below:



NRZ-I:
0 = No transition
1 = Transition at the beginning

NRZ-L:
0 = High level
1 = Low level

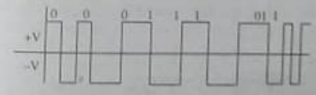
RZ:
0 = No line signal
1 = Positive or negative signal alternating.

Manchester:
0 = Transition from high to low in the middle of interval.
1 = Transition from low to high in the middle of interval.

Differential Manchester: Always transition in the middle of the interval.
0 = Transition at beginning of interval.
1 = No transition at the beginning of the interval.

Ques 28) Sketch the differential Manchester encoding for the bit stream of 0001110101. Assume the line in initially in the low state.

Ans: 4 '1' bit is indicated by the absence of a transitions at the start of interval. A '0' bit is indicated by transition at the start of the interval 2 in both case, there is a transition in the middle as well.



Ques 29) Describe the repeaters with suitable diagram.

Ans: Repeaters

Repeaters are used to connect the two or more than two similar LAN networks. Over wire it also extends the reach. While two or more networks are connected using same protocol it repeats the signals. Incoming signals (electrical, wireless or optical) are regenerated by the repeaters. When data transmission (with physical media such as Ethernet or Wi-Fi) is performed then after a limited distance, quality of the signals degrades. Repeaters are the device which preserve the signal integrity and extend the distance.

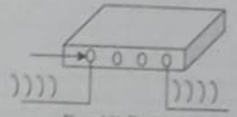


Figure 1.21: Repeaters

Ques 30) What do you understand by Hub?

Ans: Hub

Hubs act as central attachment point for network cables and hence are network connectivity devices which are positioned centrally. These are available for all guided media barring Ethernet cable. Star topology refers to the topology of a network which uses hub.

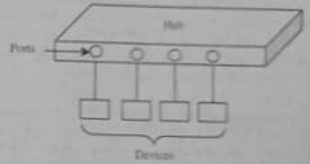


Figure 1.22: A Hub

Hubs can connect multiple communication devices as it has multiple ports. Adding or removing a device is fairly simple in hubs. Any cable break can also be easily detected.

TRANSMISSION MEDIA OVERVIEW

Ques 31) Explain the transmission media with example? And listed the Types of Transmission Media.

Or

What is bounded and unbounded media?

Or

What is guided and unguided media?

Ans: Transmission Media

The transmission media is a substance of material (solid, liquid, gas, or plasma) which propagate in energy wave form. **For example,** for receiving of sound from the ears, the transmission medium is usually air, but solids and liquids can also act as media for sound transmission.

Types of Transmission Media

The physical channel via which information is transmitted within computers in a network is referred to as **physical communication media** which may be classified as:

1) **Bounded Media:** In bounded media, the waves are conducted in a solid medium like a copper twisted wire.

Bounded Media utilises a "cabling" system which channels the data signals down a specific path.

Bounded Media may also be referred to as **Guided Media.** The data signals are bound by the "cabling" system and here cabling is used in a generic sense and does not refer to only copper wire cabling.

2) **Unbounded Media:** This is referred to as wireless transmission and includes the atmosphere and outer space. Sometimes, signals do not pass through a solid medium but pass through media like air which are not bound by a limit and are hence referred to as **unguided** or **unbounded media.** Electromagnetic energy flows easily though this media.

The unguided media does not contain a physical conductor to transmit data as it transport electromagnetic waves. It is kind of communication and often known as wireless communication. With the help of air, signals are normally broadcast and a device capable of receiving signals is also available. The wireless communication is transfer of information without the usage of wires. The distance involved may be short (a few meters as in television remote control) or long.

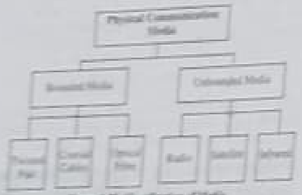


Figure 1.23: Classification of Media

Ques 32) Explain the twisted pair with physical structure and write the types of twisted pair.

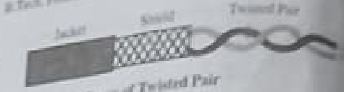
Or

Discuss about the UTP and STP in detail.

Ans: Twisted Pair Cable

This is the most economical and commonly used medium which comprises of two insulated copper wires arranged in a regular spiral pattern. A cable comprises of a number of these pairs wrapped in a tough protective casing. In twisted pair wire, a number of pairs are wrapped in a sheath of protection and these are fed into a cable.

The twisted feature helps to eliminate the crosstalk interference between adjacent pairs in a cable. The thickness of wires in a pair ranges from 0.016 to 0.036 inches and these are used mostly in systems with balanced line method of transmission.



Categories/Types of Twisted Pair

There are two types of twisted pair:

1) **Unshielded Twisted Pair (UTP):** It is commonly abbreviated as UTP. The cables without shield are known as **unshielded twisted pairs.** This cable is easy to work with and have very low cost.

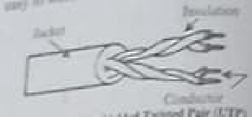


Figure 1.24: Unshielded Twisted Pair (UTP)

2) **Shielded Twisted Pair (STP):** It is usually abbreviated as STP. A cable protected with shield is called a **shielded twisted pair.** Shielded twisted pair (STP) is a copper wire and mainly used in Ethernet networks, and provide fast data rate.

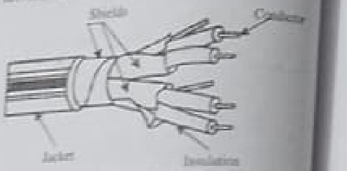


Figure 1.25: Shielded Twisted Pair (STP) Configuration

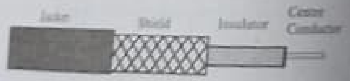
Ques 33) What do you understand by Coaxial Cables? What are the different categories of the coaxial cable?

Ans: Coaxial Cables

Coaxial cables are cables capable of carrying high-frequency range signals. Coaxial cable is also known as coax. This cable has excellent resistant to noise as protected by shield. It also has large bandwidth and low losses.

Physical Structure

The coaxial cables have two conductors. The first is situated inside an insulator, around it a shield is provided by a second conductor. It has an insulating protective coating, known as a **jacket** that covers the outer conductor. It is much less vulnerable to interference and crosstalk.



The outer shield is used to protect the external conductor from electrical signals. The materials used for insulating the inner conductor and the difference between outer conductor (shield) and the inner conductor, determine the cable's properties or impedance.

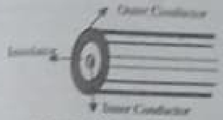


Figure 1.26: Coaxial Cables

The cable properties or impedance is determined by the distance between the outer conductor (shield) and inner conductor and the type of material used for insulating the inner conductor.

The impedances for coaxial cables are 75ohms for Cable T.V. and 50ohms for Ethernet Thinnet and Thicknet. The rate of data transfer is higher as compared to Twisted Pair cable as impedance characteristics of the cable are controlled excellently.

Types of Coaxial Cable

1) **Thinnet Cable:** A thin cable is a flexible coaxial cable that is approximately 0.64 cm (0.25 in) thick. It can be used in almost any type of network installation because this type of coaxial cable is flexible and easy to work with. Before suffering from attenuation, it can carry signals up to a distance of about 185 meters (about 607 feet).

2) **Thicknet Cable:** The thick cable is a relatively rigid coaxial cable with a diameter of about 1.27 centimeters (0.5 in). This was the first type of Ethernet in popular network architecture, so it is sometimes referred to as **Standard Ethernet.**

A thicker cable can carry a signal for 500 meters (about 1640 ft) because the copper core of a thicker cable is thicker than the core of a thinner cable. It is sometimes used as a backbone for connecting many smaller thin-based networks due to the ability of thicket to support data transfer over long distances.

Ques 34) Describe the Fiber Optics Cable with suitable diagram.

Or

Explain the Propagation Modes and types of multimode.

Ans: Optical Fiber/Fiber Optics Cable

The fibre optic cable is cable which contains tube of glass fibres within insulated casing. For long distance and high bandwidth (gigabit speed) communication such cables are designed.

By using pulses of light, fiber optic cables propagate communication signals. Irrespective of high costly, these cables are increasingly being used instead of traditional wires because it offers more capacity and is less susceptible to electrical interference. Also known as **Fiber to the Home** (FTTH), installations are becoming more common to residential areas as it provide ultra-high speed Internet service (100 Mbps and higher).

Physical Structure

Fiber optic cable is similar to coaxial cable minus the braid as is illustrated in **figure 1.27**. The centre of the fibre cable is made up of glass and propagates light. The diameter of this glass core is determined by the type of fibre used.

The diameter varies from 50 microns in multi-mode fibres to 8-10 microns in single-mode fibres. The core is surrounded by a glass **cladding** which has a lower refraction index than the core. This helps in preserving all light within the core. The cladding is protected by a thin plastic **jacket**. Fibres are grouped into bundles and protected by an outer covering.

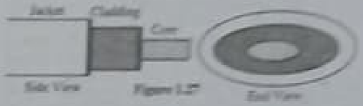


Figure 1.27

Refraction is the most important feature of Fibre Optics. This refers to the ability of a material to pass or reflect light. As light passes from one medium to another, it "bends" in the process.

An optical fiber cable has a cylindrical shape and consists of 3 concentric sections (**figure 1.28**).

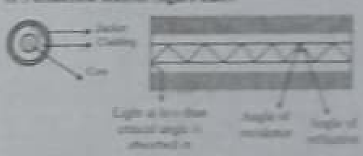


Figure 1.28: Optical Fiber Cable

1) **Core:** It is made of glass or plastic. It consists of one or more very thin strands or fibers.

2) **Cladding:** It is a glass and plastic coating and has optical properties different from core. Every fiber is surrounded by cladding.

3) **Jacket:** It made of plastic layer. Jacket is used to protect optical fiber cable against moisture, abrasion, crushing and other environmental dangers.

Propagation Modes

For propagating light along optical channels, the currently used technology supports two modes, each requiring fiber with different physical characteristics. These are given below:

1) **Single Mode:** For the cladding and core, it has separate distinct refractive indexes. With relatively few reflections off the cladding, the light ray passes through the core. For sending single source of light (one color) generally single mode is used. The core is very small and about 9 microns. Laser light is used to transmit the data.

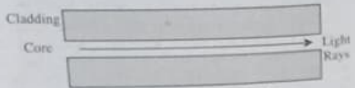


Figure 1.29: Single Mode

2) **Multimode:** In multiple modes, the light beams from a source move through the core in different paths hence named as multimode.

Types of Multimode

i) **Step Index:** Reflecting in the cladding happens inside the core. Step index has a large core so the light rays tend to bounce around. To take a longer or shorted path through the core, this causes some rays. Others bounce back and forth taking a longer path while some take the direct path with hardly any reflections. The light rays reach at the receiver end with different time interval. A signal converts itself longer than original signal. The LED light sources are used to transmit data from one end to another end. The thickness of the core is about 62.5 microns.

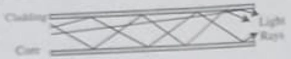


Figure 1.30: Step Index Mode

ii) **Grade Index:** In the Core's Refractive Index, it has a gradual change. Because of this, the light rays to be gradually bent back into the core path. A curved reflective path is used to represent it. It gives better results for received signal as compared to step index. The LED light sources are used for Grade index. 62.5 microns is required in typical core.

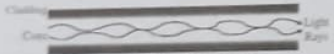


Figure 1.31: Grade Index Mode

Ques 35) Discuss about the Wireless Transmission? Also list the different unguided transmissions.

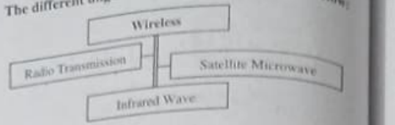
Or

Explain the Radio Waves/Radio Transmission.

Ans: Wireless Transmission

Wireless transmission is unguided media which does not establish a physical link between two or more devices and communicating without wire. Wireless signals are transmitted over the air and are received by antennas. When an antenna is connected to a wireless device then it converts the digital data into wireless signals and propagates all over its frequency range. At the other end, the receptor receives these signals and converts them back into digital data.

The different un



Radio Waves/Radio Transmission

Radio wave frequency ranges from 10 Kilohertz (kHz) to 1 Giga Hertz (GHz). These can be classified into following:

1) Short wave,
2) Very High Frequency (VHF), and
3) Ultra High Frequency (UHF).

As radio waves are omnidirectional, when an antenna transmits them, they get propagated in all directions. This implies that sending and receiving antennas need not be aligned in any particular direction to receive radio waves from each other.

Radio waves propagate in the sky mode and can travel long-long distances and thus, make it favourable for long-distance broadcasting like AM radio. Radio waves of low and medium frequencies can penetrate walls. This works as an advantage for AM radio as this ensures that it works inside buildings.

Radio waves follow the ground in VLF, LF, and MF bands as is shown in **figure 1.32(a)**.

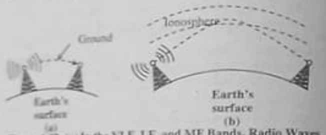


Figure 1.32: (a) In the VLF, LF, and MF Bands, Radio Waves Follow the Curvature of the Earth (b) In the HF Band, they Bounce Off the Ionosphere

In the HF and VHF bands, ground waves are absorbed by the earth. Ionosphere is the layer of charged particles which circle the earth at a height of 100 to 500km. Waves which reach this ionosphere are refracted by it and sent back to earth as illustrated in **figure 1.32(b)**. Depending on atmospheric conditions, the signals can bounce many times. Amateur radio operators (hams) and the military use the HF and VHF bands for communication.

Ques 36) Explain the Satellite Microwave Transmission and Infrared Wave Transmission.

Ans: Satellite Microwave Transmission

The satellites act as relay stations of microwaves which comprise two or more microwave transmitter/receiver pairs. These receive signal on one frequency, prepare the signal for retransmission and then send the signal on a different frequency. The frequency bands are referred to as transponders and the microwave transmitter/receiver pairs are referred to as earth stations.

The satellite microwave frequency is above 100MHz. When all energy is concentrated in a small beam using a parabolic antenna (like satellite T.V. dish), it gives a much higher signal to noise ratio. This is possible when the transmitting and receiving antennas are correctly aligned with each other.

Figure 1.33 illustrates the entire set-up:

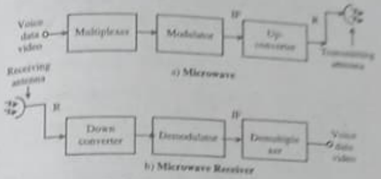


Figure 1.33: Satellite Microwave Transmitter and Receiver

As per **frequency range**, satellites may be classified into two types:

1) **C-Band:** Frequency ranges from 3.7 to 4.2 GHz and 5.9 to 6.4 GHz.
2) **Ku Band:** Frequency ranges from 11 to13 GHz.

Infrared Wave Transmission

Infrared waves are used for short range communication as they cannot infiltrate walls owing to their high frequency. This feature helps eliminate interference between one system and another. However, transmission may get disrupted by objects present between sender and receiver.

Infrared wave's frequency ranges from 300GHz to 400THz. It can be easily built at low cost without requirement of government license. Infrared communication is used in the remote control used in T.V., V.C.R. and stereos.

As infrared waves cannot penetrate walls, their security against eavesdropping is better than radio system. For indoor wireless LAN, infrared light is appropriate.

PERFORMANCE INDICATORS

Ques 37) What are the different performance indicators of a network? List them.

Or

Discuss about the Bandwidth.

Ans: Performance of a Network

Performance of a network pertains to the measure of service quality of a network as perceived by the user. There are different ways to measure the performance of a network, depending upon the nature and design of the network. The characteristics that measure the performance of a network are:

1) Bandwidth
2) Throughput
3) Latency (Delay)
4) Bandwidth - Delay Product
5) Jitter

Bandwidth

Bandwidth describes the maximum data transfer rate of a network. It measures how much data can be sent over a specific connection in a given amount of time. **For example,** a gigabit Ethernet connection has a bandwidth of 1,000 Mbps. (125 megabytes per second).

Bandwidth may refer to **bandwidth capacity** or **available bandwidth** in bit/s, which typically means the net bit rate, channel capacity or the maximum throughput of a logical or physical communication path in a digital communication system. **For example,** bandwidth test implies measuring the maximum throughput of a computer network.

Bandwidth may also refer to **consumed bandwidth** (bandwidth consumption), corresponding to achieved throughput or goodput, i.e., average data rate of successful data transfer through a communication path.

$$\text{Bandwidth} = \frac{1}{\text{BaudRate}}$$

Ques 38) Explain the Throughput with example.

Ans: Throughput

Throughput is the number of messages successfully transmitted per unit time. It is controlled by available bandwidth, the available signal-to-noise ratio and hardware limitations.

The maximum throughput of a network may be consequently higher than the actual throughput achieved in everyday consumption.

Throughput is measured by tabulating the amount of data transferred between multiple locations during a specific period of time, usually resulting in the unit of **bits per second** (bps), which has evolved to **bytes per second** (Bps), **kilobytes per second** (KBps), **megabytes per second** (MBps) and **gigabytes per second** (GBps).

For example, let us consider a highway which has a capacity of moving, say, 200 vehicles at a time. But at a random time, someone notices only, say, 150 vehicles moving through it due to some congestion on the road.

As a result, the capacity is likely to be 200 vehicles per unit time and the throughput is 150 vehicles at a time.

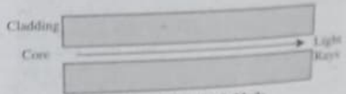


Figure 1.29: Single Mode

2) **Multimode:** In multiple modes, the light beams from a source move through the core in different paths hence named as multimode.

Types of Multimode

i) **Step Index:** Reflecting in the cladding happens inside the core. Step index has a large core so the light rays tend to bounce around. To take a longer or shorted path through the core, this causes some rays. Others bounce back and forth taking a longer path while some take the direct path with hardly any reflections. The light rays reach at the receiver end with different time interval. A signal converts itself longer than original signal. The LED light sources are used to transmit data from one end to another end. The thickness of the core is about 62.5 microns.

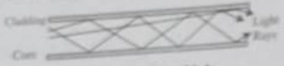


Figure 1.30: Step Index Mode

ii) **Grade Index:** In the Core's Refractive Index, it has a gradual change. Because of this, the light rays to be gradually bent back into the core path. A curved reflective path is used to represent it. It gives better results for received signal as compared to step index. The LED light sources are used for Grade index. 62.5 microns is required in typical core.

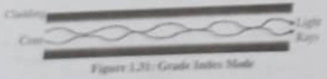


Figure 1.31: Grade Index Mode

Ques 35) Discuss about the Wireless Transmission? Also list the different unguided transmissions.

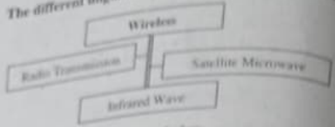
Or

Explain the Radio Waves/Radio Transmission.

Ans: Wireless Transmission

Wireless transmission is unguided media which does not establish a physical link between two or more devices and communicating without wire. Wireless signals are transmitted over the air and are received by antennas. When an antenna is connected to a wireless device then it converts the digital data into wireless signals and propagates all over its frequency range. At the other end, the receptor receives these signals and converts them back into digital data.

The different unguided transmissions are given below:



Radio Waves/Radio Transmission

Radio wave frequency ranges from 10 Kilohertz (kHz) to 1 Giga Hertz (GHz). These can be classified into following:

1) Short wave,
2) Very High Frequency (VHF), and
3) Ultra High Frequency (UHF).

As radio waves are omnidirectional, when an antenna transmits them, they get propagated in all directions. This implies that sending and receiving antennas need not be aligned in any particular direction to receive radio waves from each other.

Radio waves propagate in the sky mode and can travel long distances and thus, make it favourable for long distance broadcasting like AM radio. Radio waves of low and medium frequencies can penetrate walls. This works as an advantage for AM radio as this ensures that it works inside buildings.

Radio waves follow the ground in VLF, LF, and MF bands as is shown in **figure 1.32(a)**.

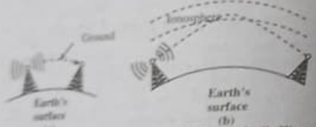


Figure 1.32: (a) In the VLF, LF, and MF Bands, Radio Waves Follow the Curvature of the Earth (b) In the HF Band, they Bounce Off the Ionosphere

In the HF and VHF bands, ground waves are absorbed by the earth. Ionosphere is the layer of charged particles which circle the earth at a height of 100 to 500km. Waves which reach this ionosphere are refracted by it and sent back to earth as illustrated in **figure 1.32(b)**. Depending on atmospheric conditions, the signals can bounce many times. Amateur radio operators (hams) and the military use the HF and VHF bands for communication.

Ques 36) Explain the Satellite Microwave Transmission and Infrared Wave Transmission.

Ans: Satellite Microwave Transmission

The satellites act as relay stations of microwaves which comprise two or more microwave transmitter/receiver pairs. These receive signal on one frequency, prepare the signal for retransmission and then send the signal on a different frequency. The frequency bands are referred to as transponders and the microwave transmitter/receiver pairs are referred to as earth stations.

The satellite microwave frequency is above 100MHz. When all energy is concentrated in a small beam using a parabolic antenna (like satellite T.V. dish), it gives a much higher signal to noise ratio. This is possible when the transmitting and receiving antennas are correctly aligned with each other.

Figure 1.33 illustrates the entire set-up:

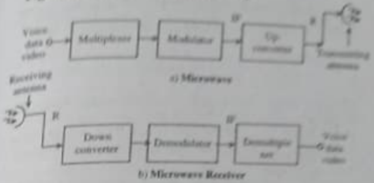


Figure 1.33: Satellite Microwave Transmitter and Receiver

As per **frequency range**, satellites may be classified into two types:

1) **C-Band:** Frequency ranges from 3.7 to 4.2 GHz and 5.9 to 6.4 GHz.

2) **Ku Band:** Frequency ranges from 11 to13 GHz.

Infrared Wave Transmission

Infrared waves are used for short range communication as they cannot infiltrate walls owing to their high frequency. This feature helps eliminate interference between one system and another. However, transmission may get disrupted by objects present between sender and receiver.

Infrared wave's frequency ranges from 300GHz to 400THz. It can be easily built at low cost without requirement of government license. Infrared communication is used in the remote control used in T.V., V.C.R. and stereos.

As infrared waves cannot penetrate walls, their security against eavesdropping is better than radio system. For indoor wireless LAN, infrared light is appropriate.

PERFORMANCE INDICATORS

Ques 37) What are the different performance indicators of a network? List them.

Or

Discuss about the Bandwidth.

Ans: Performance of a Network

Performance of a network pertains to the measure of service quality of a network as perceived by the user. There are different ways to measure the performance of a network, depending upon the nature and design of the network. The characteristics that measure the performance of a network are:

1) Bandwidth
2) Throughput
3) Latency (Delay)
4) Bandwidth - Delay Product
5) Jitter

Bandwidth

Bandwidth describes the maximum data transfer rate of a network. It measures how much data can be sent over a specific connection in a given amount of time. **For example**, a gigabit Ethernet connection has a bandwidth of 1,000 Mbps, (125 megabytes per second).

Bandwidth may refer to **bandwidth capacity** or **available bandwidth** in bit/s, which typically means the net bit rate, channel capacity or the maximum throughput of a logical or physical communication path in a digital communication system. **For example**, bandwidth test implies measuring the maximum throughput of a computer network.

Bandwidth may also refer to **consumed bandwidth** (bandwidth consumption), corresponding to achieved throughput or goodput, i.e. average data rate of successful data transfer through a communication path.

$$\text{Bandwidth} = \frac{1}{\text{BaudRate}}$$

Ques 38) Explain the Throughput with example.

Ans: Throughput

Throughput is the number of messages successfully transmitted per unit time. It is controlled by available bandwidth, the available signal-to-noise ratio and hardware limitations.

The maximum throughput of a network may be consequently higher than the actual throughput achieved in everyday consumption.

Throughput is measured by tabulating the amount of data transferred between multiple locations during a specific period of time, usually resulting in the unit of **bits per second (bps)**, which has evolved to **bytes per second (Bps)**, **kilobytes per second (KBps)**, **megabytes per second (MBps)** and **gigabytes per second (GBps)**.

For example, let us consider a highway which has a capacity of moving, say, 200 vehicles at a time. But at a random time, someone notices only, say, 150 vehicles moving through it due to some congestion on the road.

As a result, the capacity is likely to be 200 vehicles per unit time and the throughput is 150 vehicles at a time.

Ques 38) What do you mean by Latency? And define the propagation or Transmission Time.

Or

What do you understand the Queuing Time and processing delay?

Ans: Latency

Latency may be defined as the time required to successfully sending a packet across a network.

It is measured in many ways like round trip, one way, etc.

1) It might be affected by any component in the chain which is utilised to vehiculate data, like workstations, WAN links, routers, LAN, servers and eventually may be limited for large networks, by the speed of light.

Latency = Propagation Time + Transmission Time + Queuing Time + Processing Delay

Where the terms are:

1) **Propagation Time:** It is the time required for a bit to travel from the source to the destination.

   Propagation time = Distance / Propagation speed

2) **Transmission Time:** Transmission time is a time based on how long it takes to send the signal down the transmission line.

   Transmission time = Message size / Bandwidth

3) **Queuing Time:** Queuing time is a time based on how long the packet has to sit around in the router.

4) **Processing Delay:** Processing delay is the delay based on how long it takes the router to figure out where to send the packet.

Ques 40) Describe the Bandwidth-delay product and write the cases.

Ans: Bandwidth-Delay Product

Bandwidth and delay are two performance measurements of a link. However, what is significant in data communications is the product of the two, the bandwidth-delay product.

Let us take two hypothetical cases as examples.

Case 1: Assume a link is of bandwidth 1bps and the delay of the link is 5s. Let us find the bandwidth-delay product in this case. From the image, we can say that this product 1 × 5 is the maximum number of bits that can fill the link. There can be close to 5 bits at any time on the link.

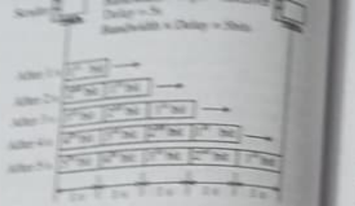


Figure 1.34

Case 2: Assume a link is of bandwidth 3bps. From the image, we can say that there can be a maximum of 3 × 5 = 15 bits on the line. The reason is that, at each second, there are 3 bits on the line and the duration of each bit is 0.33s.

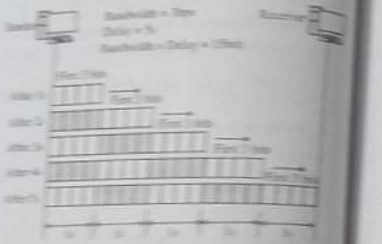


Figure 1.35

For both examples, the product of bandwidth and delay is the number of bits that can fill the link. This estimation is significant in the event that we have to send data in bursts and wait for the acknowledgement of each burst before sending the following one. To utilize the maximum ability of the link, we have to make the size of our burst twice the product of bandwidth and delay. Also, we need to fill up the full-duplex channel. The sender ought to send a burst of data of (2*bandwidth*delay) bits. The sender at that point waits for the receiver's acknowledgement for part of the burst before sending another burst. The amount 2*bandwidth*delay is the number of bits that can be in transition at any time.

Module 2

Data Link Layer

DATA LINK LAYER

Ques 1) Define data link layer. What are the data link layer design issues? Discuss them.

Or

What do you mean by flow control and error control?

Ans: Data Link Layer

Data Link Layer is the second layer of the OSI model. The data-link layer is responsible for error free transfer of data frames. This layer provides synchronisation for the physical level. The purpose of the data link layer is to transfer blocks of data without error between two adjacent devices. Adjacent devices are physically connected by a communication channel such as telephone lines, coaxial cables, optical fibers, or satellites. Data link layer deals with two basic issues:

1) How data frames can be reliably transmitted, and
2) How a shared communication medium can be accessed.

Data Link Layer Design Issues

The design issues of the data link layer are given below:

1) **Services Provided to Network Layer:** The function of the data link layer is to provide services to the network layer. The principle service is transferring data from the network layer on the source machine to the network layer on the destination machine.

   The job of the data link layer is to transmit the bits to the destination machine, so they can be handed over to the network layer. The actual transmission follows the path but it is easier to think in terms of two data link layer processes communicating using a data link protocol. The data link layer can be designed to offer various services. The actual services offered can vary from system to system.

2) **Framing:** The data link layer needs to pack bits into frames, so that each frame is distinguishable from another. Framing is the function of the data link layer that separates a message from one source to a destination or from other messages to other destinations, by adding a sender address and a destination address.

   The destination address defines where the packet is to go; the sender address helps the recipient acknowledge the receipt.

   i) **Fixed-Size Framing:** Frames can be of fixed or variable size. In fixed-size framing, there is no need for defining the boundaries of the frame; the size itself can be used as a delimiter. An example of this type of framing is the ATM wide-area network, which uses frames of fixed size called **cells**.

   ii) **Variable-Size Framing:** In Variable-Size Framing, one needs a way to define the end of the frame and the beginning of the next. Historically, two approaches were used for this purpose:

   a) **Character-Oriented Protocols:** In a Character-oriented Protocol, data to be carried are 8-bit characters from a coding system such as ASCII. **Figure 2.1** shows the format of a frame in a character-oriented protocol.

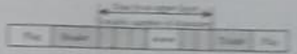


Figure 2.1: Frame in Character-oriented Protocol

   Character-oriented framing was popular when only text was exchanged by the data link layers. The flag could be selected to be any character not used for text communication.

   b) **Bit-Oriented Protocols:** In a Bit-oriented Protocol, the data section of a frame is a sequence of bits to be interpreted by the upper layer as text, graphic, audio, video and so on. However, in addition to headers (and possible trailers), still need a delimiter to separate one frame from the other. Most protocols use a special 8 bit pattern flag 01111110 as the delimiter to define the beginning and the end of the frame, as shown in **figure 2.2**.

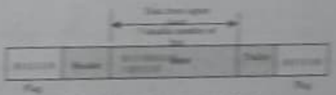


Figure 2.2: Frame in a Bit-oriented Protocol

3) ***Flow Control:*** *Flow control is a set of procedures that tells the sender how much data it can transmit before it must wait for an acknowledgment from the receiver. The flow of data must not be allowed to overwhelm the receiver. Any receiving device has a limited speed at which it can process incoming data and a limited amount of memory in which to store incoming data.*

For flow control there is two approaches are commonly used:

i) **Feedback-Based Flow Control:** In this approach receiver sends back information to the sender giving it permission to send more data or at least telling the sender how the receiver is doing.

ii) **Rate-Based Flow Control:** In this the protocol has a built-in mechanism that limits the rate at which senders may transmit data, without using feedback from the receiver. The two categories of flow control are:

a) Stop-and-Wait
b) Sliding Window

4) **Error Control:** Error control provides error detection and correction. There are two basic strategies for dealing with errors. These are:

i) To include only enough redundancy to allow the receiver to confirm that an error occurred, but not aware of which error and therefore request it for re-transmission.

ii) Second method is to include enough unwanted data along with each block of data sent to enable to receiver to extract what the transmitted character must have been.

Mechanics for **error handling** at this layer are based on error detection and retransmission with the error handling usually performed using algorithms implemented in software such as checksum in error detection and correction.

Ques 2) What is Error? And also write the type of Errors.

Ans: Error

Error is a condition when the output information does not match with the input information. During transmission, digital signals suffer from noise that can introduce errors in the binary bits travelling from one system to other. That means a 0 bit may change to 1 or a 1 bit may change to 0.

If there is a change in one data stream (a bit) which is transferred and received, then error occurs. **For example,** if 1 is transferred and 0 is received or reverse of it.

Types of Errors

There are two types of errors are occurred in digital transmission systems:

i) **Single-bit Errors:** If there is a change in a single bit then the error is known as 'single bit error' i.e., 1 is changed to 0 or vice versa. In other words, in a single bit error, only single bit is changed.

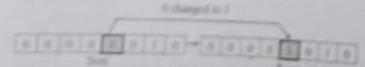


Figure 2.3: Single-Bit Error

ii) **Burst/Multiple-bit Errors:** Whenever two or more bits are changed in a given stream then this error is known as **burst errors**. This type of error is also known as **multiple-bit errors**.

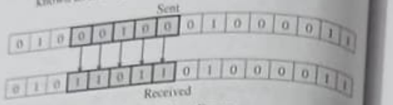


Figure 2.4: Burst Error

Ques 3) Describe the error detection and correction with example.

Or

Define the parity check and Cyclic Redundancy Check (CRC).

Or

Explain the different error detecting and correcting methods?

Or

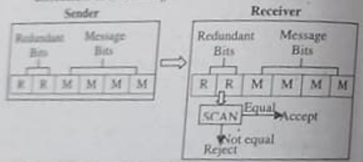
Write short notes on the following:

1) Parity Checks
2) Checksum

Ans: Error Control Methods/Techniques

Following are the techniques of error control:

1) **Error Detection:** The method of verification of the received message whether correct or not, is known as 'error detection'. This does not depend on the original message. At the receiver's end, the correctness of the message is determined by checking the redundant bits which are added into the sent message. In this method, the parity bits are checked which predicts the correctness of the message.



Error Detecting Methods/Techniques

The common codes for error detection are as follows:

i) **Parity Checking:** Parity checking is the commonly used and less expensive method of error detection. In this method, the parity bit which is known as 'redundant bit' is added to every data stream so that the total 1's in the stream become even.

The parity bit is checked in the blocks of data at the sender's end. Following are the two methods to add the parity bit:

a) If it contains odd number of 1's then parity of 1 is added to it.

b) If it contains even number of 1's then 0 is added to it.

Whenever the block of data is received at the receiver's end, the parity is computed and compared with received parity bit for checking the correctness of the data.

For example, let us consider the data is 1010001. As it contains odd number of 1's (3) then parity bit with value 1 is associated with data in order to make even number of 1's. It is added to left of the data. After adding these 1's the data to be transmitted will be 11010001. In case of odd parity checking, the zero is added to left of the data to be sent, i.e., it becomes 01010001.

If the data contains even number of 1's (like 1101001), then 1 is associated to the left of the data in order to make odd number of 1's. Thus data that is to be transmitted becomes 11101001. If data transferred is not correct then parity bit becomes incorrect. This shows that there is an error during the data transmission.

ii) **Cyclic Redundancy Check or Block Check Characters:** CRC method is used to check the errors that occurred in the data transmission. This technique uses a complex calculation in order to generate a number according to the data transmitted. Before transmission, the calculation is performed by sending device and then result is transmitted to receiving device.

The similar calculation is also performed by receiving device whenever the transmission is done. If the sending and receiving devices both find the same output then this shows that no error occurred during the transmission. This scheme is known as 'redundancy check' as it contains the redundant values (extra value) along with the data. This extra value is known as 'error-checking value'. This method is most commonly used for the error free synchronous data transmission. IBM uses the CRC-16 for the CRC method. A constant "divisor" is used by this method and it can have the following form:

1000 1000 0001 00001

This method consists of the following **steps**:

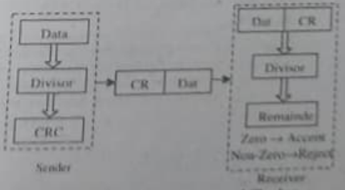


Figure 2.5: CRC Generator and Checker

a) Divisor – 1 bits are added after least significant bit of the message that is to be transferred. The message is recorded and transmitted. The extra bits are transferred first (i.e., most significant bits).

b) The exclusive ORed operation is performed with the divisor and 16 most significant bits of the message. The extra bits are taken from the message and then added to result to generate another 16 bits of data headed by 1.

c) The exclusive ORed operation is also performed with the remaining process till all the bits in the message are not exhausted.

d) The result generated after the exclusive OR operation is the CRC characters. Sufficient numbers of leading zeros are added to the CRC character in order to form 16 bits.

iii) **Checksum:** In checksum method, data is divided into **k** segments and every segment contains **m** bits.

The segments are added with the help of 1's complement arithmetic in order to find out the sum at the sender's end. Next the result obtained is complemented to find out the checksum. The checksum obtained is associated with data segments and then sent to receiver as shown in **figure 2.6(a)**.

Similar process is also followed at the sender's end and sum is calculated at the receiver's end. The sum obtained is complemented. In case the result is zero or one (complete) then this shows that received data is accepted as shown in **figure 2.6(b)**. While if the result is not zero then this shows that result is rejected. Consider the following **example** where an original data is given. In this data value of k=4 (group of digits) and m=8 (digit in every group).

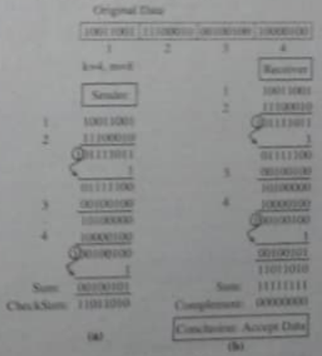


Figure 2.6

Checksum will detect both odd as well as even number of bits.

2) **Error Correction:** After error detection, the error is to be corrected. For this, error correcting codes are used to correct the error occurred in the message which is detected at the receiver's end. Sometimes the data is to be resent for correcting the errors.

Hamming distance code is the best known method of error correction.

Ques 4) Discuss about the Hamming Code.

Ans: Hamming Code
Hamming codes are used for detecting and correcting single bit errors occurred during the data transmission. Hamming code word is derived from the name of scientist **R. W. Hamming**.

Hamming distance code can be used to identify and correct the single bit error occurred within the transmitted block of data. Numbers k and n can be used to identify the errors. So, the hamming code is (n, k). Modulo 2 arithmetic is employed in the hamming distance codes. The n shows the block length and k shows the message length.

Hamming code is characterised by the following structure:

$$(n,k)=(2^m-1,\ 2^m-1-m)$$

Where m = 2, 3,.... Hamming code has a minimum distance of 3.

Exclusive OR logic operation replaces addition in modulo 2 arithmetic. The truth table for this operation is shown in **table 2.1**.

Table 2.1: Truth Table for XOR

A	B	A ⊕ B
0	0	0
0	1	1
1	0	1
1	1	0

The Hamming code format for four data bits would be:
$D_7\ D_6\ D_5\ P_4\ D_3\ P_2\ P_1$ → 7-bits code

Where, the D-bits are the data bits and the P-bits are the parity bits. P_1 is set so that it establishes even parity over bits 1, 3, 5 and 7 (P_1, D_3, D_5 and D_7). P_2 is set for even parity over bits 2, 3, 6 and 7 (P_2, D_3, D_6 and D_7). P_4 is set for even parity over bits 4, 5, 6 and 7 (P_4, D_5, D_6 and D_7).

The above concept can be extended to any number of bits. A 15-bit code, e.g., would have the following format:
$D_{15}, D_{14}, D_{13}, D_{12}, D_{11}, D_{10}, D_9, P_8, D_7, D_6, D_5, P_4, D_3, P_2,$
P_1 → 15-bit code

Note: Parity bits are inserted at each 2^n bit. This is true for Hamming codes of any length.

Ques 5) Let us suppose the message frame 1101011011 for which the divisor is 10011. Compute the CRC.

Ans: After adding the four bits (1 less than the divisor) in the frame it becomes 11010110110000. Whenever the division operation is performed, the remainder is 1110. Thus the CRC is 1110 and transmitted frame is 11010110111110.

Frame: 1101011011
Generator: 10011

Message After Appending Four Zero Bits
11010110110000

```
             1100001010
10011 ) 11010110110000
        10011
         10011
         10011
          00001
          00000
           00010
           00000
            00101
            00000
             01011
             00000
              10110
              10011
               01010
               00000
                10100
                10011
                 01110
                 00000
remainder   →     1110
```

Figure 2.7: Calculation of CRC

Transmitted Frame: 11010110111110

Ques 6) Explain how CRC is used in detecting errors for the following polynomial: $G(x) = x^4 + x + 1$. Consider the information sequence 1101011011.

i) Find the codeword corresponding to the above sequence.

ii) Suppose the left most bit is inverted due to the noise on transmission link on the above message. What is the result of receivers CRC calculation? How does the receiver know that are error has occurred?

Ans: Divisor, $g(x) = x^4 + x + 1 = 10011$
Message, m = 1101011011
Message after appending Four Zero Bits (1 less than the divisor): 11010110110000

Transmitted Frame = 11010110110000	Received Frame = 11010110111110
1100001010 10011) 11010110110000 10011 10011 10011 00001 00000 00101 00000 01011 00000 10110 10011 01010 00000 10100 10011 01110 00000 **Calculation of CRC** 1110	1100001010 10011) 11010110111110 10011 010011 10011 000001 00000 00010 00000 00101 00000 01011 00000 10111 10011 001001 00000 10011 10011 **Checking of Error** 00000 00000

In figure above, the zero remainder shows that the data is transmitted correctly.

Now after inverting the leftmost bit of the message, i.e., 01010110111110, the final answer will not be 00000 which will show that an error has occurred.

Ques 7) Data bits 1011 must be transmitted. Construct even-parity, 7-bit, Hamming code for this data.

Ans: P_1 must be a 1 in order for bits 1, 3, 5, and 7 to be even parity.
P_2 must be a 0 in order for bits 2, 3, 6 and 7 to be even parity.
P_4 must be a 0 in order for bits 4, 5, 6 and 7 to be even parity.

Therefore, the final code is:

D_7	D_6	D_5	P_4	D_3	P_2	P_1
1	0	1	0	1	0	1

The Hamming code data are now ready for transmission and reception. At the receiving end, they are decoded to see if any errors have occurred. Bits 1, 3, 5 and 7; bits 2, 3, 6, and 7; and bits 4, 5, 6, and 7 are all checked for even-parity. Should they check out, there is no error? However, should there be an error, the problem bit can be located by forming a 3-bit binary number out of the three parity checks.

Ques 8) Let us suppose that the data bits 1011 are to be transmitted. Determine how many even parity, 7 bit and hamming code is required for such data transmission.

Ans:
1) P_1 must be a 1 in order for bits 1, 3, 5, and 7 to be even parity.
2) P_2 must be a 0 in order for bits 2, 3, 6, and 7 to be even parity.

3) P_4 must be a 0 in order for bits 4, 5, 6, and 7 to be even parity.

Thus, the final code will be as follows:

D_7	D_6	D_5	P_4	D_3	P_2	P_1
1	0	1	0	1	0	1

The hamming code data now obtained can be easily transmitted and received. The data received at the receiver end is checked in order to see whether an error has occurred or not. For even parity, bits 1, 3, 5 and 7, bits 2, 3, 6, and 7, and bits 4, 5, 6, and 7 are checked. The problem bit can be determined by making a 3-bit binary number out of the three parity checks, if an error is found. If no error has occurred then this shows that data is transmitted correctly.

SLIDING WINDOW PROTOCOLS

Ques 9) Discuss the different categories of flow control protocols.

Or

Explain the following flow control protocols:
1) Stop-and-Wait
2) Sliding Window

Ans: Categories of Flow Control
1) **Stop-and-Wait Protocol:** In stop-and-wait protocol, the source sends a packet and only after receiving the acknowledgement from the destination, it sends next packet. This is a simple protocol, but it results in lots of delay, and the bandwidth is not used efficiently.

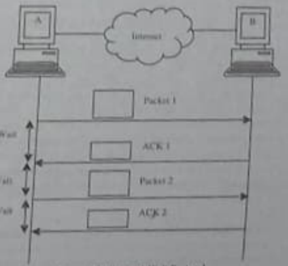


Figure 2.7: Stop-and-Wait Protocol

When the source (end system A) sends the first packet to the destination (end system B) and waits for the acknowledgment, then B sends an acknowledgement packet. Then A sends the second packet, and B sends the acknowledgement. A repeat this process until sender A transmit an end of transmission frame (EOT). The process is illustrated in **figure 2.4**. A **refinement** to this protocol is the sliding window protocol.

2) **Sliding Window Protocol:** In the elementary data link protocols, data frames are transmitted in one direction only but there is a need to transmitting data in both directions. This is achieved by sliding window protocol. In the sliding window method, the sender can transmit several frames before needing an acknowledgment. Frames can be sent one right after another, meaning that the link can carry several frames at once and its capacity can be used efficiently.

The sender maintains information about:
i) Size of sender window,
ii) Last acknowledgement received,
iii) Last frame sent.

The receiver acknowledges only some of the frames, using a single ACK to confirm the receipt of multiple data frames.

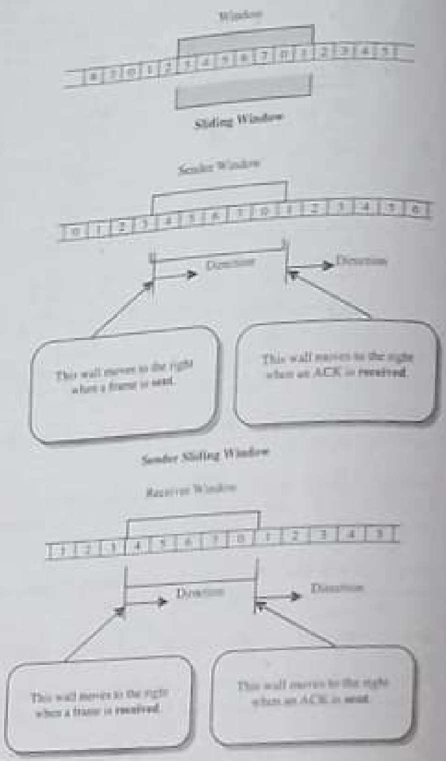
Receiver holds information about:
i) Receiver window size,
ii) Large acceptable frame,
iii) Last frame received.

In the sliding window method protocol, several frames can be in transit at a time. The sliding window refers to imaginary boxes at both the sender and the receiver. This window can hold frames at either end and provides the upper limit on the number of frames that can be transmitted before requiring an acknowledgment.

Frames may be acknowledged at any point without waiting for the window to fill up and may be transmitted as long as the window is not yet full. To keep track of which frames have been transmitted and which received, sliding window introduces an identification scheme based on the size of the window. The frames are numbered modulo-n, which means they are numbered from 0 to n – 1.When the receiver sends an ACK, it includes the number of the next frame it expects to receive. The window can hold n – 1 frames at either end; therefore, a maximum of n – 1 frames may be sent before an acknowledgement is required. **Figure 2.8** shows the relationship of a window to the main buffer.

For example, figure 2.8 shows a sample transmission that uses sliding window flow control with a window of seven frames. In this example, all frames arrive undamaged. There are two steps as given below for implementation:

Step 1: When data 0 and data 1 are sent by the sender, sliding window of the sender shrank from the left. The receiver received the data 0 and data 1 and then sliding window of the receiver shrank from the left.



Window
6 7 0 1 2 3 4 5 6 7 0 1 2 3 4 5
Sender Window
0 1 2 3 4 5 6 7 0 1 2 3 4 5 6
Direction
Direction
This wall moves to the right when a frame is sent.
This wall moves to the right when an ACK is received.
Receiver Window
1 2 3 4 5 6 7 0 1 2 3 4 5
Direction
Direction
This wall moves to the right when a frame is received.
This wall moves to the right when an ACK is sent.

Sliding Window

Sender Sliding Window

Figure 2.8: Receiver Sliding Window

Step 2: When acknowledgement is sent by receiver for data 0 and data 1, the sliding window of receiver is expanded to the right. The sender received the acknowledgement for data 0 and data 1 and then the sliding window of sender expanded from the right.

Similarly we repeat Step 1 and Step2 for transmitting data 2 from sender to the receiver and transmitting acknowledgement from the receiver to the sender. Again we will repeat the same process for data 3, data 4 and data 5 as well as for acknowledgement 6.

Types of Sliding Window Protocols
The Sliding Window ARQ (Automatic Repeat request) protocols are of two categories:
i) Go – Back – N ARQ
ii) Selective Repeat ARQ

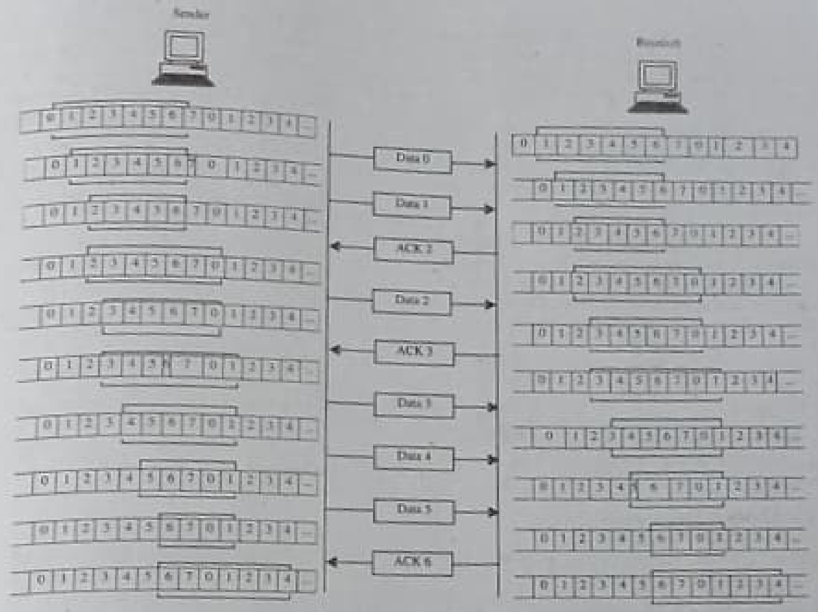


Figure 2.9: Example of Sliding Window

Ques 10) What is ARQ? Write the different types of ARQ techniques?

Or

Discuss about Stop-and-Wait ARQ and Sliding Window ARQ with suitable diagram.

Or

Explain the different types of Sliding Window ARQ.

Or

Write short notes on the following protocols:
1) **Go-Back-N ARQ**
2) **Selective Request ARQ**

Ans: Automatic Repeat Request (ARQ)
Automatic Repeat Request (ARQ), also known as **Automatic Repeat Query**, is an error-control method for data transmission that uses acknowledgements (messages sent by the receiver indicating that it has correctly received a data frame or packet) and timeouts (specified periods of time allowed to elapse before an acknowledgment is to be received) to achieve reliable data transmission over an unreliable service.

If the sender does not receive an acknowledgment before the timeout, it usually re-transmits the frame/packet until the sender receives an acknowledgment or exceeds a predefined number of re-transmissions.

The receiver will send back an ARQ message to the transmitter to indicate that the last block should be retransmitted.

Types of ARQ Techniques
There are two commonly used ARQ techniques:
1) **Stop-and-Wait ARQ:** Stop-and-wait ARQ is a form of stop-and-wait flow control extended to include retransmission of data in case of lost or damaged frames. It is also known as **ABP(Alternating Bit Protocol).** For retransmission to work, four features are added to the basic flow control mechanism:
i) The sending device keeps a copy of the last frame transmitted until it receives an acknowledgment for that frame. Keeping a copy allows the sender to retransmit lost or damaged frames until they are received correctly.

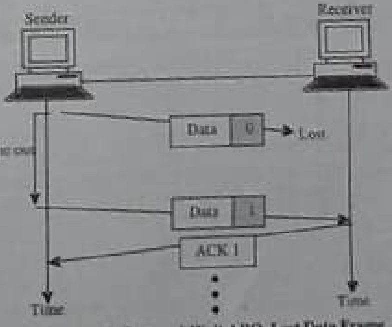


Figure 2.10: Stop-and-Wait ARQ, Lost Data Frame

ii) For identification purposes, both data frames and ACK frames are numbered alternately 0 and 1. This numbering allows for identification of data frames in case of duplicate transmission.

iii) If an error is discovered in a data frame, indicating that it has been corrupted in transit, a NAK frame is returned. NAK frames, which are not numbered, tell the sender to retransmit the last frame sent (Figure 2.11).

iv) The sending device is equipped with a timer. If an expected acknowledgment is not received within an allotted time period, the sender assumes that the last data frame was lost in transit and sends it again (Figure 2.8 and Figure 2.11).

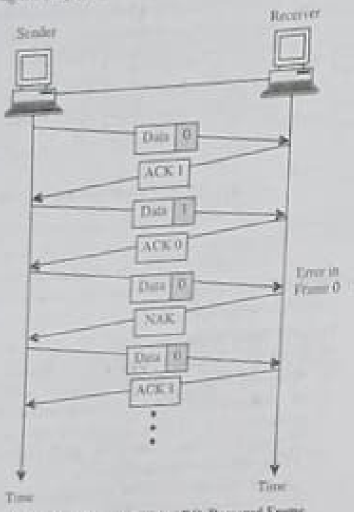


Figure 2.11: Stop-and-Wait ARQ, Damaged Frame

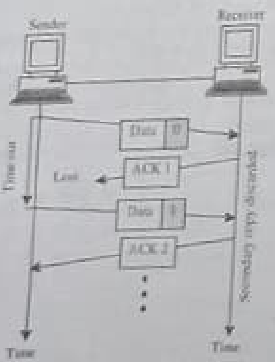


Figure 2.12: Stop-and-Wait ARQ, Lost ACK Frame

2) **Sliding Window ARQ:** It is of two types:

i) **Go-Back-n ARQ:** This is a specific instance of the automatic repeat request (ARQ) protocol, in which the sending process continues to send a number of frames specified by a window size even without receiving an acknowledgement (ACK) packet from the receiver.

It is a special case of the general sliding window protocol with the transmit window size of N and receive window size of 1.

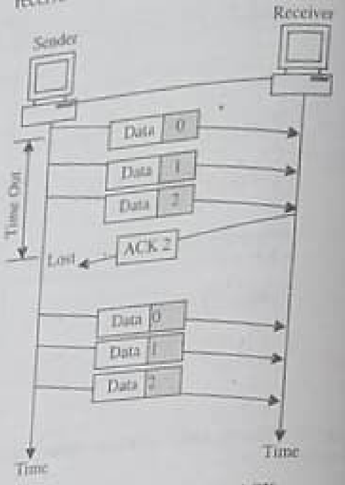


Figure 2.13: Go-back-n, lost ACK

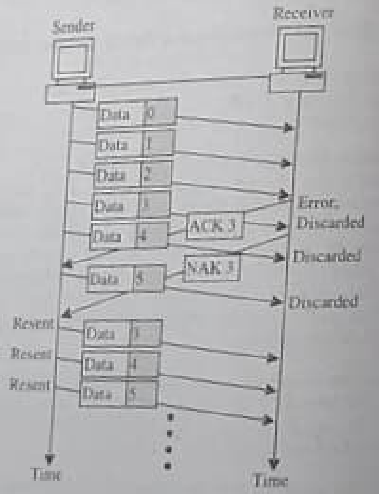


Figure 2.14: Go-back-n, damaged data frame

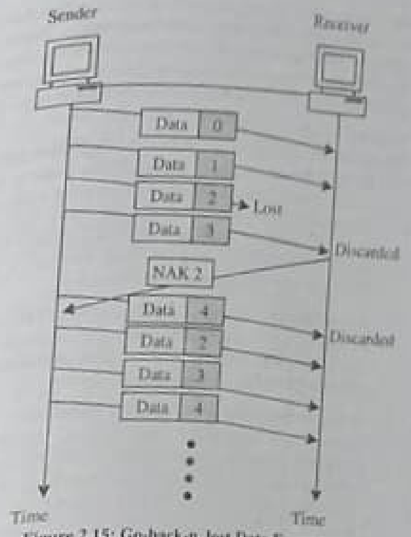


Figure 2.15: Go-back-n, lost Data Frame

ii) **Selective Reject ARQ:** Selective Reject or Selective Repeat is one of the automatic repeat-request (ARQ) techniques. With selective repeat, the sender sends a number of frames specified by a window size even without the need to wait for individual ACK from the receiver as in stop-and-wait. However, the receiver sends ACK for each frame individually, which is not like cumulative ACK as used with go-back-n.

The receiver accepts out-of-order frames and buffers them. The sender individually retransmits frames that have timed out. In selective-repeat ARQ, only the specific damaged or lost frame is retransmitted. If a frame is corrupted in transit, a NAK is returned and the frame is resent out of sequence. The receiving device must be able to sort the frames it has and insert the retransmitted frame into its proper place in the sequence.

The receiving device must contain sorting logic to enable it to reorder frames received out of sequence. It must also be able to store frames received after a NAK has been sent until the damaged frame has been replaced. The sending device must contain a searching mechanism that allows it to find and select only the requested frame for retransmission.

A buffer in the receiver must keep all previously received frames on hold until all retransmissions have been sorted and any duplicate frames have been identified and discarded. To aid selectivity, ACK numbers, like NAK numbers, must refer to the frame received (or lost) instead of the next frame expected.

This complexity requires a smaller window size than is needed by the go-back-n method if it is to work efficiently. It is recommended that the window size be less than or equal to (n+1)/2, where n – 1 is the go-back-n window size. **Figure 2.16** of selective repeat, damaged data frame is **shown above.**

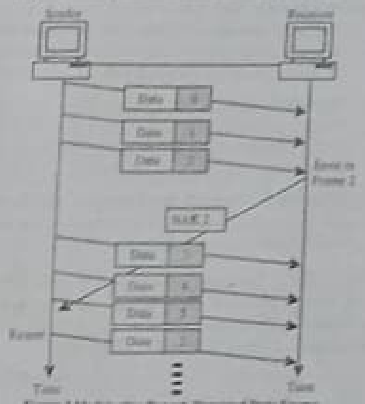


Figure 2.16: Selective Repeat, Damaged Data Frame

Ques 11) What is difference between Selective-Reject and Go-Back-N

Ans: Difference between Selective-Reject and Go-Back-N

The difference between Selective-Reject and Go-Back-N is shown in **table 2.3**.

Table 2.3: Selective Reject vs. Go-Back-N

Basis	Selective Reject	Go-Back-N
Retransmission	Selective Retransmission	Unnecessary retransmissions in case of lost packets
Complexity	More complex than Go back N	Less complex
Simplicity	Not very simple to implement	simple to implement
Throughput	Lesser throughput	Gives more throughput in case of significant end-to end transmission delay

HIGH-LEVEL-DATA LINK CONTROL(HDLC)

Ques 12) Discuss HDLC? What are the different types of stations? Also explain the Transfer Modes of HDLC.

Or

Explain the working of high-level data link control (HDLC).

Or

Differentiate between normal and asynchronous balanced modes of operations in HDLC. **(2018-2021[03])**

Ans: HDLC

High-level Data Link Control is an International Standards Organisation data link protocol. All these **bit-oriented protocols** grew out from the original IBM SDLC **(Synchronous Data Link Control).**

HDLC is a discipline for the management of information transfer over a data communication channel. HDLC has a basic structure that governs the function and the use of control procedures.

Types of Stations

To satisfy a variety of applications, HDLC defines three types of stations. These are:

1) **Primary Station:** It has the responsibility for controlling the operation of the link. Frames issued by the primary are called **command**.

2) **Secondary Station:** It operates under the control of the primary station. Frames issued by a secondary are called **responses**. The primary maintains separate logical links with each secondary station of the line.

3) **Combined Station:** It combines the features of primary and secondary. A combined station may issue both commands and responses.

Since, HDLC has been defined as a general purpose data link control protocol. The stations can be configured in different network configurations as (all configurations are illustrated in **figure 2.17, 2.17** (a) and (b)):

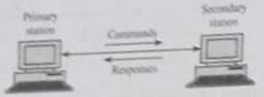
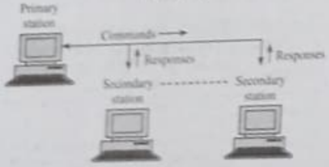
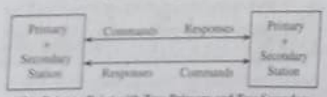


Figure 2.17: Point to Point with Single Primary and Secondary (Point-to-Point Link)



(a): Multipoint with Single Primary and Multiple Secondary (Multipoint Link)



(b): Point to Point with Two Primary and Two Secondary (Point-to-Point Link between Combined Stations)

Figure 2.18

The frames sent by primary station to the secondary station are known as commands and those from the secondary to the primary as responses. Two configurations shown in part (1) and (2) have a single primary station are known as **unbalanced configurations**. Unbalanced configuration supports both full duplex and half duplex transmission.

The configuration in part (3) has two primary stations and is known as **balanced configuration**. Balanced configuration supports both full duplex and half duplex transmission. Since each station has both a primary and a secondary, they are also known as combined stations.

Transfer Modes of HDLC

The data transfer can be in one of the following three modes:

1) **Normal Response Mode (NRM):** This mode is used in unbalanced configuration. The primary node will initiate the data transfer, but the secondary node can send data only on command from the primary node. NRM is used for communication between a host computer and the terminals connected to it.

2) **Asynchronous Balanced Mode (ABM):** This mode is used with balanced configuration. A combined node can initiate transmission. ABM is used extensively for point-to-point full-duplex communication.

3) **Asynchronous Response Mode (ARM):** This mode is used with unbalanced configuration. The primary node will have the responsibility to initiate the link, error recovery, and logical disconnection, but the secondary node may initiate data transmission without permission from the primary. ARM is rarely used.

Difference between Normal and Asynchronous Balance Modes of Operations

Table 2.4 shows the difference between Normal and Asynchronous Balance Modes of operations:

Table 2.4: Difference between Normal and Asynchronous Balance Modes

Normal Response Mode	Asynchronous Balance Modes
The secondary must wait for permission from the primary before transmitting any frames.	In this mode, we use combined stations and each end can just go ahead and send frames without permission from anyone else.
Normal Response Mode is used most frequently in multi-point lines, where the primary station controls the link.	It is mainly used in point-to-point links, for communication between combined stations.
This is the main mode in use.	Asynchronous Balanced Mode is not used widely today.

Ques 13) Explain frames types of HDLC?

Or

What is the frame format of HDLC?

Or

Draw the different frame formats in HDLC. (2019[03])

Ans: Frames Types

In HDLC both data and control messages are carried in a standard format frame. Three classes of frame are used in HDLC:

1) **Unnumbered Frames (U-Frames):** These are used for functions such as link setup and disconnection. The name derives from the fact that they do not contain any acknowledgement information, which is contained in sequence numbers.

2) **Information Frames (I-Frames):** These carry the actual information or data and are normally referred to simply as I-frames. They can be used to piggy back acknowledgement information relating to the flow of I-frames in the reverse direction when the link is being operated in ABM or ARM.

3) **Supervisory Frames (S-Frames):** These are used for error and flow control and hence contain send and receive sequence numbers.

Frame Format in HDLC

The frame format of HDLC is shown in **figure 2.19**.

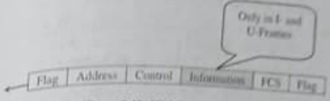


Figure 2.19: HDLC – Frame Format

The functions of each field are as follows:

1) **Flag Field:** This field of an HDLC frame is an 8-bit sequence with a bit pattern of 01111110. It identifies both the beginning and end of a frame and serves as a synchronisation pattern for the receiver.

2) **Address Field:** This field contains the address of the secondary station. If a primary station creates a frame, it contains to address. If a secondary creates the frame, it contains from address. An address field can be 1 byte or several bytes long, depending on the network. One byte of address can identify upto 128 stations.

3) **Control Field:** This field is a 1 or 2 byte segment of the frame used for flow and error control.

4) **Information Field:** This field contains the user's data from the network layer or network management information. Its length can vary from one network to another but is always fixed within each network.

5) **Frame Check Sequence (FCS):** FCS in an error detection field. It contains either a 2- or 4-byte.

MEDIUM ACCESS CONTROL (MAC) SUBLAYER

Ques 14) What is MAC (Medium Access Control) sub layer? Explain its features.

Ans: MAC (Medium Access Control) Sub Layer

Protocols used to determine who goes next on a multi access channel belong to sub-layer of the data link layer called the MAC. Medium Access Control (MAC) protocol is used to provide the basic functionality of data link layer of the Ethernet LAN system. MAC sub-layer is mainly concerned with media access strategies and is different for different LANs. It supports different types of transmission media at different data rates.

Features of MAC/LLC

1) Controls the access to the shared channel in autonomous DTEs.

2) Provides a scheme that reduces a LANS susceptibility to errors.

3) Provides a more compatible interface with WANS, since the LLC is a subset of the equivalent portion of the WAN standard.

4) The LLC is independent of access method, whereas MAC is protocol specific. This gives the 802 network a flexible interface into and out of the LAN.

Ques 15) What is the structure of MAC?

Ans: Structure of MAC

The structure of MAC is divided into **preamble**, **header** and **CRC** (**cyclic redundancy check**).

1) **Preamble:** The purpose of the idle time before transmission starts is to allow a small time interval for the receiver electronics in each of the nodes to settle after completion of the previous frame. A node starts transmission by sending an 8 byte (64 bit) preamble sequence. This consists of 62 alternating 1's and 0's followed by the pattern 11.

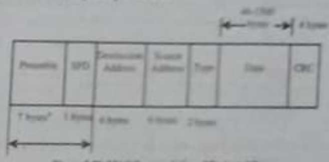


Figure 2.20: MAC Encapsulation of Packet of Data

The last byte, which finished with the "11", is known as the **"Start of Frame Delimiter"** (SFD). It warns the station or stations that this is the last chance for synchronisation. When encoded using Manchester encoding, at 10 Mbps, the 62 alternating bits produce a 5 MHz square wave.

The purpose of the preamble is to allow time for the receiver in each node to achieve lock of the receiver Digital Phase Lock Loop which is used to synchronise the receive data clock to the transmit data clock.

2) **Header:** The header consists of three parts:

   i) **Destination Address:** A 6-byte destination address, which specifies a single recipient node (unicast mode), a group of recipient nodes (multicast mode), or the set of all recipient nodes (broadcast mode).

   ii) **Source Address:** A 6-byte source address, which is set to the sender's globally unique node address. This may be used by the network layer protocol to identify the sender, but usually other mechanisms are used. Its main function is to allow address learning, which may be used to configure the filter tables in a bridge.

   iii) **Type:** A 2-byte type field, which provides a Service Access Point (SAP) to identify the type of protocol being carried (e.g. the values 0x0800 is used to identify the IP network protocol, other values are used to indicate other network layer protocols). In the case of IEEE 802.3 LLC, this may also be used to indicate the length of the data part.

3) **Cyclic Redundancy Check (CRC):** The 32-bit CRC added at the end of the frame provides error detection in the case where line errors (or transmission collisions in Ethernet) result in corruption of the MAC frame. Any frame with an invalid CRC is discarded by the MAC receiver without further processing. The MAC protocol does not provide any indication that a frame has been discarded due to an invalid CRC.

Ques 16) Define the various multiple access control protocols.

Or

Write note on ALOHA and CSMA. (2021[05])

Ans: Multiple Access Protocols

Many algorithms for allocating a multiple access channel are known. Protocols which are used in allocating a multiple access channel are given below:

1) **ALOHA:** "ALOHA refers to a simple communications scheme in which each source (transmitter) in a network sends data whenever there is a frame to send."

If the frame successfully reaches the destination (receiver), the next frame is sent. If the frame fails to be received at the destination, it is sent again. ALOHA protocol is a main **contention protocol** (Access to the medium from many entry points is called **contention**. It is controlled with a contention protocol).

In a wireless broadcast system or a half-duplex two-way link, ALOHA works perfectly.

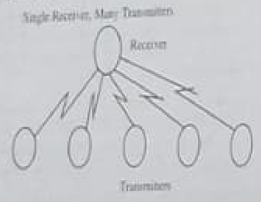


Figure 2.20: Satellite System, Wireless (ALOHA Protocol)

To minimise the number of collisions, thereby optimising network efficiency and increasing the number of subscribers that can use a given network, a scheme called slotted ALOHA was developed. This system employs signals called **beacons** that are sent at precise intervals and tell each source when the channel is clear to send a frame.

Further improvement can be realised by a more sophisticated protocol called Carrier Sense Multiple Access with Collision Detection (CSMA/CD).

Types of ALOHA

There are two types of ALOHA protocol:

i) ***Pure Aloha Protocol:*** With Pure ALOHA (**figure 2.21**), stations are allowed access to the channel whenever they have data to transmit. Because the threat of data collision exists, each station must either monitor its transmission on the rebroadcast or await an acknowledgment from the destination station.

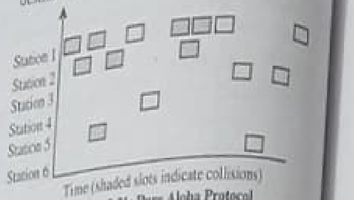
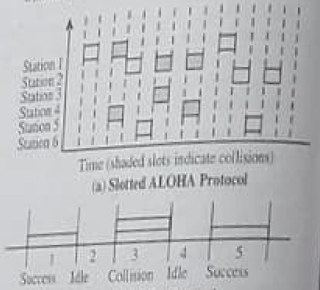


Figure 2.21: Pure Aloha Protocol

ii) **Slotted ALOHA Protocol:** By making a small restriction in the transmission freedom of the individual stations, the throughput of the ALOHA protocol can be doubled. Assuming constant length packets, transmission time is broken into slots equivalent to the transmission time of a single packet. Stations are only allowed to transmit at slot boundaries.



(a) Slotted ALOHA Protocol

(b) Slotted ALOHA Protocol

Figure 2.22

When packets collide they will overlap completely instead of partially. This has the effect of doubling the efficiency of the ALOHA protocol and has come to be known as Slotted ALOHA (**figure 2.22(a) and (b)**).

2) **Carrier Sense Multiple Access (CSMA): "Carrier Sense"** describes the fact that a transmitter listens for a carrier wave before trying to send.

That is, it tries to detect the presence of an encoded signal from another station before attempting to transmit.

If a carrier is sensed, the station waits for the transmission in progress to finish before initiating its own transmission. "**Multiple Access**" describes the fact that multiple stations send and receive on the medium. Transmissions by one node are generally received by all other stations using the medium.

Carrier Sense Multiple Access (CSMA) improves performance when there is a higher medium utilisation. When a NIC has data to transmit, the NIC first listens to the cable (using a transceiver) to see if a carrier (signal) is being transmitted by another node.

This may be achieved by monitoring whether a current is flowing in the cable. The individual bits are sent by encoding them with a 10 (or 100 MHz for Fast Ethernet) clock using Manchester encoding.

Data is only sent when no carrier is observed (i.e., no current present) and the physical medium is therefore idle. Any NIC, which does not need to transmit, listens to see if other NICs have started to transmit information to it.

However, this alone is unable to prevent two NICs transmitting at the same time. If two NICs simultaneously try transmitting, then both could see an idle physical medium (i.e. neither will see the other's carrier signal), and both will conclude that no other NIC is currently using the medium.

Ques 17) How does pure aloha and slotted aloha differ? (2019[03])

Ans: Difference between Pure Aloha and Slotted Aloha

Table 2.5 shows the difference between Pure Aloha and Slotted Aloha:

Table 2.5: Difference between Pure Aloha and Slotted Aloha

Pure Aloha	Slotted Aloha
In this aloha, any station can transmit the data at any time.	In this, any station can transmit the data at the beginning of any time slot.
In this, The time is continuous and not globally synchronized.	In this, The time is discrete and globally synchronized.
In Pure Aloha, Probability of successful transmission of data packet $= G \times e^{-2G}$	In Slotted Aloha, Probability of successful transmission of data packet $= G \times e^{-G}$
In pure aloha, Maximum efficiency = 18.4%	In slotted aloha, Maximum efficiency = 36.8%
Pure aloha does not reduce the number of collisions to half.	Slotted aloha reduces the number of collisions to half and doubles the efficiency of pure aloha.

Ques 18) Explain the working of CSMA/CD? (2019[03])

Ans: CSMA with Collision Detection (CSMA/CD)

The CSMA/CD specifications have been standardized by IEEE 802.3 standard. A second element to the Ethernet access protocol is used to detect when a collision occurs. When there is data waiting to be sent, each transmitting NIC also monitors its own transmission. If it observes a collision (excess current above what it is generating, i.e., > 24 mA for coaxial Ethernet), it stops transmission immediately and instead transmits a 32-bit jam sequence.

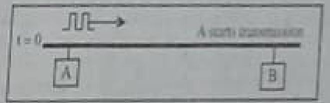
The purpose of this sequence is to ensure that any other node, which may currently be receiving this frame, will receive the jam signal in place of the correct 32-bit MAC CRC; this causes the other receivers to discard the frame due to a CRC error. To ensure that all NICs start to receive a frame before the transmitting NIC has finished sending it, Ethernet defines a minimum frame size (i.e. no frame may have less than 46 bytes of payload).

The minimum frame size is related to the distance, which the network spans, the type of media being used and the number of repeaters, which the signal may have to pass through to reach the furthest part of the LAN. Together these define a value known as the Ethernet Slot Time, corresponding to 512 bit times at 10 Mbps.

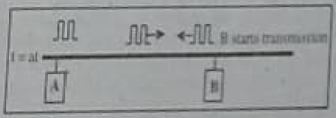
For example, when two or more transmitting NICs each detect a corruption of their own data (i.e., a collision) each responds in the same way by transmitting the jam sequence.

The following sequence depicts a collision:

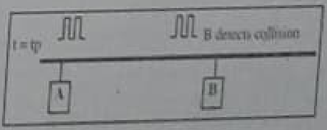
1) At time t=0, a frame is sent on the idle medium by NIC.



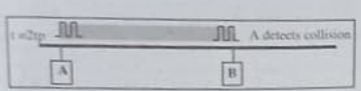
2) A short time later, receiver NIC also transmits. (In this case, the medium, as observed by the receiver NIC happens to be idle too).



3) After a period, equal to the propagation delay of the network, the receiver NIC detects the other transmission from sender, and is aware of a collision, but sender NIC has not yet observed that receiver NIC was also transmitting. Receiver continues to transmit, sending the Ethernet Jam sequence (32 bits).



4) After one complete round trip propagation time (twice the one way propagation delay), both NICs are aware of the collision. Receiver will shortly cease transmission of the Jam Sequence; however sender will continue to transmit a complete Jam Sequence. Finally the cable becomes idle.



Ques 19) Write note on CSMA/CA. (2021[02])

Or

How collision is avoided in CSMA/CA? Describe the different strategies used for this. (2018[05])

Ans: Collision Avoidance in CSMA/CA

Carrier Sense Multiple Access/with Collision Avoidance (CSMA/CA) is a network contention protocol used for carrier transmission in networks using the 802.11 standard. In contrast to the Carrier Sense Multiple Access/Collision Detect (CSMA/CD) protocol, which handles transmissions only after a collision has taken place, CSMA/CA works to avoid collisions prior to their occurrence.

CSMA/CA increases network traffic as it requires sending out a signal to the network even before transmitting any real data. This is to listen for any collision scenarios in the network and to inform other devices not to transmit.

Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) is the least popular of the access methods. In CSMA/CA, a computer will signal its intention to transmit before it actually transmits data. In this way, computers will sense when a collision might occur; this allows them to avoid transmission collisions. Unfortunately, this broadcasting of the intention to transmit data increases the amount of traffic on the cable and slows down network performance. This access method was once a popular method in the Macintosh environment and is now used with WLANs.

It is particularly important for wireless networks, where the collision detection of the alternative CSMA/CD is unreliable due to the hidden node problem. CSMA/CA is a protocol that operates in the Data Link Layer (Layer 2) of the OSI model.

Strategies for Collision Avoidance

Collisions are avoided through the use of CSMA/CA's three strategies: the **interframe space**, the **contention window**, and **acknowledgment**, as shown in **figure 2.23**.

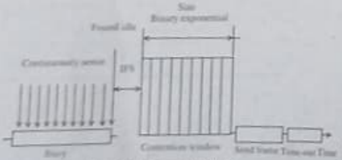


Figure 2.23: Timing in CSMA/CA

1) **Interframe Space (IFS):** First, collisions are avoided by deferring transmission even if the channel is found idle. When an idle channel is found, the station does not send immediately. It waits for a period of time called the interframe space or IFS. Even though the channel may appear idle when it is sensed, a distant station may have already started transmitting.

The distant station's signal has not yet reached this station. The IFS time allows the front of the transmitted signal by the distant station to reach this station. If after the IFS time the channel is still idle, the station can send, but it still needs to wait a time equal to the contention time. The IFS variable can be used to prioritize station or frame types. **For example**, a station that is assigned a shorter IFS has a higher priority.

In CSMAICA, the IFS can also be used to define the priority of a station or a frame.

2) **Contention Window:** The contention window is an amount of time divided into slots. A station that is ready to send chooses a random number of stores as it wait time. The number of slots in the window changes according to the binary exponential back-off strategy.

This means that it is set to one slot the first time and then doubles each time the station cannot detect an idle channel after the IFS time.

In CSMA/CA, if the station finds the channel busy, it does not restart the timer of the contention window; it stops the timer and restarts it when the channel becomes idle.

3) **Acknowledgment:** With all these precautions, there still may be a collision resulting in destroyed data. In addition, the data may be corrupted during the transmission. The positive acknowledgement and the time-out timer can help guarantee that the receiver has received the frame.

Ques 20) Describe the channel allocation problem.

Or

Write short notes on the following:

i) **Static Channel Allocation**

ii) **Dynamic Channel Allocation**

iii) **Hybrid Channel Allocation**

Ans: Channel Allocation Problem

Allocating a single broadcast channel among competing users is called **channel allocation**. Channel allocation deals with the allocation of channels to cells in a cellular network. Once the channels are allocated, cells may then allow users within the cell to communicate via the available channels. In other words, certain protocols are needed to allow each user to communicate without interference. Even though there are variety of practices, channel allocation can be better achieved either by static or dynamic approach.

Types of Channel Allocation

There are two types of channel allocation as:

1) **Static Channel Allocation in LANs and MANs:** The traditional way of allocating a single channel, such as a telephone trunk, among multiple competing users is

Frequency Division Multiplexing (FDM). If there are N users, the bandwidth is divided into N equal sized portions, each user being assigned one portion.

Since each user has as private frequency band, there is no interference between users. When there are only a small and fixed number of users, each of which has a heavy (buffered) load of traffic (e.g., carries' switching offices), FDM is a simple and efficient allocation mechanism.

The poor performance of static FDM can easily be seen from a simple queuing theory calculation.

Let Mean time delay = T

Capacity of Channel = C bps

Arrival rate = λ frames/sec

Exponential probability density function = 1/ bits/frame

With these parameters the arrival rate is λ frames/sec and the service rate is μC frames/sec. From the queuing theory it can be shown that for Poisson arrival and service times,

$$T = \frac{1}{\mu C - \lambda}$$

Now lets divide the single channel into N independent sub-channels, each with capacity C/N bps. The mean input rate on each of the sub-channels will now be λ/N. Recomputing T we get

$$T_{FDM} = \frac{1}{\mu(C/N) - (\lambda/N)} = \frac{N}{\mu C - \lambda} = NT$$

2) **Dynamic Channel Allocation in LANs and MANs:** The five key assumptions of dynamic channel allocation in LANs and MANs are given below:

i) **Station Model:** The model consists of N independent stations (computers, telephones, personal communicators, etc.), each with a program or user that generates frames for transmission. The probability of a frame being generated in an interval of length Δt is λΔt, where λ is a constant (the arrival rate of new frames). Once a frame has been generated, the station is blocked and does nothing until the frame has been successfully transmitted.

ii) **Single Channel Assumption:** A single channel is available for all communication. All stations can transmit on it and all can receive from it. As far as the hardware is concerned, all stations are equivalent, although protocol software may assign priorities to them.

iii) **Collision Assumption:** If two frames are transmitted simultaneously, they overlap in time and the resulting signal is garbled. This event is called a **collision**. All stations can detect collisions. A collided frame must be transmitted again later. There are no errors other than those generated by collisions.

iv) **Continuous Time:** Frame transmission can begin at any instant. There is no master clock dividing time into discrete intervals.

v) **Slotted Time:** Time is divided into discrete intervals (slots). Frame transmissions always begin at the start of a slot. A slot may contain 0, 1, or more frames, corresponding to an idle slot, a successful transmission, or a collision, respectively.

vi) **Carrier Sense:** Station can tell if the channel is in use before trying to use it. If the channel is sensed as busy, no station will attempt to use it until it goes idle.

vii) **No Carrier Sense:** Station cannot sense the channel before trying to use it. Thy just go ahead and transmit. Only later can they determine whether or not the transmission was successful.

3) **Hybrid Channel Allocation in LANs and MANs:** The third category of channel allocation methods includes all systems that are hybrids of fixed and dynamic channel allocation systems. Several methods have been presented that fall within this category and in addition, a great deal of comparison has been made with corresponding simulations and analyses.

ETHERNET

Ques 21) Write a note on LAN/MAN standards.

Ans: LAN/MAN Standards

Institute of Electrical and Electronic Engineers (IEEE) issue numerous widely accepted LAN-recommended standards. Because they encourage the use of common approaches for LAN protocols and interfaces, hence these standards are very important.

The following standards are accepted and organized by IEEE LAN committees (**table 2.6**):

Table 2.6

IEEE LAN Standard	System
IEEE 802.1	Architecture, Management and Internet Working
IEEE 802.2	Logical Link Control
IEEE 802.3	Ethernet Working Group (e.g., CSMA/CD)
IEEE 802.4	Token Bus
IEEE 802.5	Token Ring
IEEE 802.6	Metropolitan Area Networks
IEEE 802.7	Broadband LANs
IEEE 802.8	Fiber Optic LANs
IEEE 802.9	Integrated Data and Voice Networks
IEEE 802.10	Security
IEEE 802.11	Wireless Networks

Under ISO 8802, the IEEE standards are gaining wide acceptance, and the International Organization for Standards (ISO) is accepting the 802 standards. The maximum number of manufacturers and vendors are manufacturing and marketing equipment that fulfill these standards and procedures of promoting open systems and networks.

To keep the OSI model and the 802 standards as compatible as possible, the IEEE 802 standards and committees play major role. 802 divides the data link layer into two sub layers namely:

1) Logical Link Control (LLC) and
2) Medium Access Control (MAC)

Figure 2.24 shows the overall relationship among the 802 standards and ISO model.

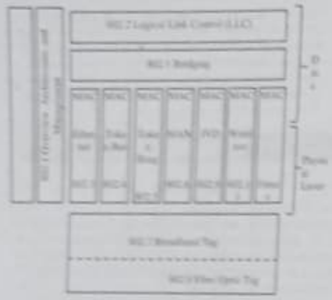


Figure 2.24: IEEE LAN Standards

Ques 22) Discuss IEEE 802.3 standard in detail.

Or

What is Ethernet? What is the frame format of Ethernet?

Or

Draw and explain the frame format for Ethernet. (2018[03])

Or

Describe the frame format for IEEE 802.3 standard in detail. (2022[03])

Ans: IEEE 802.3 Standards: Ethernet

Ethernet provides high speed data with low cost. Its installation is easy. Because of such advantages, they are widely accepted in the computer market and have the capacity to support virtually all popular network protocols. Today, Ethernet is an ideal networking technology for maximum computer users.

An Ethernet standard known as **IEEE Standard 802.3** is developed by IEEE institute. For configuring an Ethernet network, this standard defines rules and specifies procedures in what way the elements interact with one another. Network equipment and network protocols can communicate efficiently by adhering to the IEEE standard.

Frame Format of Ethernet

Following are the frame format of Ethernet:

7 bytes	1 byte	2 or 6 bytes	2 bytes	4-1500 bytes			4 bytes	
				(Data / Pad)				
Preamble	Start Frame Delimiter	Dest MAC address	Length	DSAP	SSAP	CTRL	FCS	NLI

1) **Preamble:** To allow the transmitter and receiver to synchronize their communication, this stream of bits is used. Preamble is a pattern of binary 56 ones and zeroes arranged in alternative way. The preamble is immediately followed by Start Frame Delimiter.

2) **Start Frame Delimiter:** This is in the form of 10101011 and is used to show the beginning of the frame information.

3) **Destination MAC:** This is the MAC address of the machine receiving data.

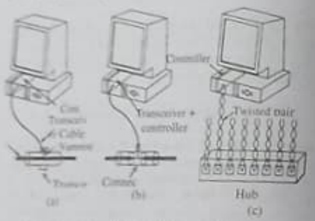


Figure 2.25: Three Kinds of Ethernet Cabling (a) 10Base5 (b) 10Base2 (c) 10Base-T

4) **Source MAC:** For the machine transmitting data, this is the MAC address.

5) **Length:** It is represented in bytes. This indicates the length of the whole Ethernet frame. While this field can hold some value among 0 and 65,534, this rarely larger than 1500 as that is usually the maximum frame size for serial connections. An Ethernet network is used to connect serial devices to access the internet.

6) **Data/Padding (Payload):** This field is used the data insertion. If you are running IP over Ethernet, it is where the IP header and data is placed. If you are running IPX/SPX (Novell), this field contains IPX information. The frame has four particular fields:
   i) **DSAP** - Destination Service Access Point
   ii) **SSAP** - Source Service Access Point
   iii) **CTRL** - Control bits for Ethernet Communication
   iv) **NLI** - Network Layer Interface

7) **FCS:** This field is reserved for the Frame Check Sequence (FCS) which is determined by Cyclic Redundancy Check (CRC). The FCS permits Ethernet to find out the errors in the Ethernet frame and reject the frame if damaged.

Ques 23) What is the standard Ethernet? Discuss them.

Ans: Standard Ethernet

The Standard Ethernets has four categories which depend on cable used to connect the network as shown in **figure 2.26**.

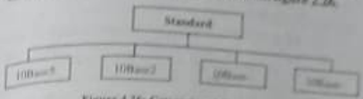


Figure 4.26: Categories of Standard Ethernet

1) **10Base5:** The 10Base5 cable is basically known as **thicker Ethernet**. The notation is 10Base5 and operates at 10Mbps. It is used in baseband signalling and also can provide segment up to 500 meters. The first number of 10Base5 shows the speed in Mbps.

   The term baseband comes from "Base" (or "BASE"). This shows that transmission is a broadband type.

2) **10Base2:** The 10Base2 or thin Ethernets are very flexible to bend very easily. In addition, thinner Ethernet is much cheaper and easier to install, but it can only run for 185 meters per segment while it can handle only 30 machines each.

3) **10Base-T:** Problems associated with a 10Base5 cable breakdown lead the system to a different wiring pattern, in which all stations are like cables running on a central hub, in which they are all electrically connected. However, all these wires are used by the telephone company, as most office buildings are already wired this way, and in many ways, additional pairs are usually available. This method is known as 10Base-T. It does not buffer traffic at the hub.

4) **10Base-F:** 10Base-F uses the fiber optics. This is expensive in the market due to the cost of connectors and terminators, but has excellent noise immunity and is also the method of choice when moving between widely separated hubs.

   It can be useful for several km distances. Wiretapping fiber wire-tapping is much more complex than copper wire hence it also provides good security protection.

The following table describes the main characteristics of **Ethernet cable** options:

	10BASE5	10BASE2	10BASE-T	10BASE-F
Transmission Medium	Coaxial cable (50 ohm)	Coaxial cable (50 ohm)	Unshielded twisted pair	850-nm optical fiber pair
Signalling Technique	Baseband (Manchester)	Baseband (Manchester)	Baseband (Manchester)	Manchester/ On-off
Topology	Bus	Bus	Star	Star
Maximum Segment Length (m)	500	185	100	500
Nodes Per Segment	100	30	—	33
Cable Diameter	10 mm	5 mm	0.4 to 0.6 mm	62.5/125 mm

Ques 24) What is the responsibility of Ethernet MAC sublayer?

Ans: Responsibility of Ethernet MAC Sublayer

The two primary responsibilities of Ethernet MAC are as given below:

1) **Data Encapsulation:** Data encapsulation provides three primary functions:
   i) Frame Delimiting,
   ii) Addressing, and
   iii) Error Detection.

   Data encapsulation procedure contains frame before transmission and after receiving them. The MAC layer adds a header and trailer to the layer 3 PDU in the frame. In the transmission of bits as they placed on the media and in grouping of bits at receiving node, the use of frames supports.

2) **Media Access Control:** The replacement of frames on the media and the removal of frames from the media is the function of MAC sublayer. It manages the media access control as its name implies. It contains initiation of frame transmission and recovery from transmission failure due to collisions.

Ques 25) What do you understand by Fast Ethernet? Also write the Fast Ethernet Goals.

Ans: Fast Ethernet

Fast Ethernet is a type of Ethernet standards that can carry traffic at a nominal rate of 100 Mbit/s as compared to standard Ethernet speed of 10 Mbit/s. 100BaseTX (T = "twisted" pair copper) hardware supports 100 megabyte Ethernet standards.

Sometimes full-duplex fast Ethernet is mentioning "200 Mbit/s", while this is certainly misleading because the level of improvement will only be achieved when traffic patterns are symmetric.

1) Logical partitioning of fast Ethernet adapters into **Media Access Controller** (MAC) deals with high-level issues of medium availability.

2) PHY stands for **Physical Layer-Interfaced.** A 4-bit 25MHz synchronous parallel interface is used to connect MAC and PHY. This is known as media-independent interface (MII). When a two-bit 50 MHz version is used to link PHY and MAC then it is called as low media independent interface (RMII).

3) Repeaters are also allowed to connect multiple PHYs for their various interfaces.
4) There is usually a network adapter between ICs or a connection between ICs, but MII can rarely be an external connection.
5) MII is the interface between MAC and PHY, using this assumption, the specification are written.
6) MII is used to fix the theoretical maximum data bit rate for all versions of fast internet at 100 Mbit/s.
7) The **Data Signalling Rate** measured is less than the maximum seen on a real network due to the required headers and trailers (addressing and error-detection bits) on each frame, the "lost frame" due to noise after every transmission.

Fast Ethernet Goals

The goals of fast Ethernet are as discussed below:
1) Upgrade the data rate to 100 Mbps.
2) Make it compatible with Standard Ethernet.
3) Keep the same 48-bit address.
4) Keep the same frame format.
5) Keep the same minimum and maximum frame lengths.

Ques 26) Explain the Physical Layer of Fast Ethernet.

Or

Write short notes on the following:
i) **100BASE-TX**
ii) **100BASE-FX**
iii) **100BASE-T2**
iv) **100BASE-BX**

Ans: Physical Layer of Fast Ethernet

Fast Ethernet is divided into two versions which are as follows:
1) **Copper:** 100BASE-T is one of Fast Ethernet standards for twisted pair cable. It consists of:
   i) 100BASE-TX (100 Mbit/s over two-pair Cat5 or better cable),
   ii) 100BASE-T4 (100 Mbit/s over four-pair Cat3 or better cable)
   iii) 100BASE-T2 (100 Mbit/s over two-pair Cat3 or better cable). The section length is limited to 100 meters (328 ft) for a 100BASE-T cable (with 10BASE-T and Gigabyte Ethernet). All standards come under IEEE 802.3.

The implementations or installations of 100BASE-T are done with 100BASE-TX. Versions of 100BASE-T are given below:
i) **100BASE-TX:** It is the main form of Fast Ethernet and runs on two wire-pairs within a Category 5. Like 10BASE-T, suitable pairs are the orange and green pairs in the TIA / EIA-568-B termination standards, T568A or T568B. These pairs use 1, 2, 3 and 6 pins.

RJ-45 Wiring (TIA/EIA-568-B T568B)			
Pin	Pair	Wire	Color
1	2	1	White/orange
2	2	2	Orange
3	3	1	White/green
4	1	2	Blue
5	1	1	White/blue
6	3	2	Green
7	4	1	White/brown
8	4	2	Brown

Each segment of the network can achieve a maximum distance of 100 meters. In this configuration, it uses a pair of twisted wires in each direction, providing 100 Mbit/s throughput in each direction.

ii) **100BASE-T4:** The early implementation of Fast Ethernet was 100BASE-T4. This requires four twisted copper pairs, but those pairs require only category 3 instead of Category 5 for TX, while only one pair is reserved for transmission, one to receive and the remaining two to change direction.

It is very unusual 8B6T code which is used to convert 8 bits data into 6 base-3 digit. The two resulting 3-digit base-3 symbols are sent parallel to 3 pairs using 3-level pulse-amplitude modulation (PAM-3).

iii) **100BASE-T2:** The data transmitted at 4 bits per symbol with two copper pairs in the 100BASE-T2.

A 4-bit symbol is extended to two 3-bit symbols through a non-trivial scrambling process which is based on a linear feedback shift register. This is necessary to flatten the emission spectrum and the bandwidth of the signal, as well as to compare the transmission line using its properties.

The mapping of the original bits in the symbol code is sometime variable and has a fairly large duration. Following table shows the final mapping of symbols to PAM-5 line modulation levels.

Symbol	Line Signal Level
000	0
001	+1
010	–1
011	–2
100(ESC)	+2

2) **Fiber:** There are three versions of fiber:
   i) **100BASE-FX:** One version of Fast Ethernet is 100BASE-FX optical fiber. It transmits 1300nm near-infrared (NIR) light wavelengths through two elements one to receive (RX) and the other to transmit (TX). The maximum length of a half-duplex connection is 400 m (1,310 ft) or 2 km (6,600 ft) for full duplex on multimode optical fibers. It should be possible to travel long distances when using single-mode optical fiber. Similar to 100BASE-TX, 100BASE-FX uses the same 4B5B encoding and NRZI line code. It should use SC, ST, or MIC connectors as being the preferred option. 100BASE-FX optical fiber is not compatible with the 10 MBit/s version of 10BASE-FL.

   ii) **100BASE-SX:** There is a version of Fast Ethernet over optical fiber. Two varieties of multimode optical fibers are used to transmit and receive. It is an alternative to low-cost 100BASE-FX because it uses short-wavelength fiber optics that is significantly less expensive than long-wavelength optics used in 100BASE-FX. The 100BASE-SX can work well at distances up to 300 meters (980ft).

   Unlike 10BASE-FL, 100BASE-SX optical fiber uses the same wavelength, the 10 MBit/s versions over optical fiber. This allows existing media to be optimized for 850nm transmission but needs to be upgraded at both ends at the same time, as coding and signaling are not compatible.

   Shorter distances and shorter wavelengths (850nm) can be supported by it. The 100BASE-SX uses cheaper optical components (LEDs instead of lasers), making it easier those upgrading from 10BASE-FL.

   iii) **100BASE-BX:** 100BASE-BX over a single strand is a version of optical fiber for fast Ethernet (unlike 100BASE-FX, which uses a pair of fibers). Single-mode fibers are used with a special multiplexer, which transmits signals and receives wavelengths.

Ques 27) What is Gigabit Ethernet?

Or

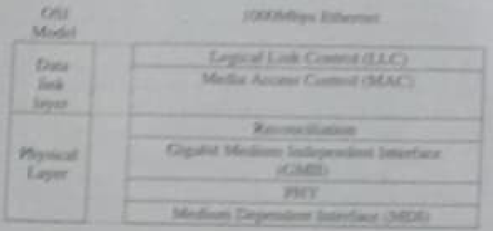
***List the features of Gigabit Ethernet.* (2019[03])**

Ans: Gigabit Ethernet

World's most popular and widespread networking technology is Ethernet. The latest version of Ethernet is Gigabit Ethernet which is 100 times faster than the standard Ethernet because it provides 1000Mbps (1Gbps) bandwidth. Still this is compatible with present Ethernet because it uses the CSMA / CD and MAC protocols.

Since year 1970's, Ethernet is most widespread networking technology in the world. There was approximate 82% Ethernet of the total networking equipment in use in 1996. IEEE approved the Fast Ethernet Standard in 1995 which offers that 10 time's larger bandwidth and added new features like full-duplex operation and auto-negotiation. In this, the Ethernet established as a scalable technology and it is expected to scale even further with the emerging Gigabit Ethernet standard.

At starting, it is required to be deployed Ethernet as a backbone in present networks. This may be used to aggregate traffic between clients and "server farms" and for linking fast Ethernet switches. This may be also used for interconnecting workstations and servers for high bandwidth applications like CAD or medical imaging. Gigabit Ethernet provides 1000Mbps speed and is the third generation Ethernet technology. This offer higher speeds and fully compatible with existing Ethernets. The performance of existing networks will be able to upgrade without changing existing wiring or protocols. The existing technologies such as ATM and FDDI are expected to provide high speed data using Gigabit Ethernet. Shows that the layered structure of the Gigabit Ethernet and is described under physical layer and MAC layer:


OSI Model
1000Mbps Ethernet
Data link layer
Physical Layer
Logical Link Control (LLC)
Media Access Control (MAC)
Reconciliation
Gigabit Medium Independent Interface (GMII)
PHY
Medium Dependent Interface (MDI)

Features of Gigabit Ethernet
1) Gigabit Ethernet provides a seamless migration path that fully protects investment in existing network infrastructure. Gigabit Ethernet will retain IEEE 802.3 and Ethernet frame formats and 802.3 managed object specifications, enabling organizations to retain existing cable, operating system, protocol, desktop applications while upgrading to gigabit performance Program and network management strategies and tools.
2) Relative to the original Fast Ethernet, FDDI, ATM and other backbone solutions, Gigabit Ethernet provides an optimal path. At least for the moment, it is a reliable and cost-effective way to improve connectivity between switches and switches and between switches and servers. Network designers can build high-speed infrastructures that efficiently use high-speed, mission-critical applications and file backup. Network managers will provide users with faster access to the Internet, intranets, metropolitan and wide area networks.
3) The IEEE 802.3 working group has set up 802.3z and 802.3ab Gigabit Ethernet working groups whose mission is to develop Gigabit Ethernet standards that meet different needs. The standard supports full duplex and half duplex 1000Mbps, the corresponding operation using IEEE 802.3 Ethernet frame format and CSMA / CD media access control methods. Gigabit Ethernet is also backwards compatible with 10BaseT and 100BaseT. In addition, the IEEE standard will support multimode fiber up to 550 meters, single mode fiber up to 70 kilometers and copper cable up to 100 meters. Gigabit Ethernet fills the gap with 802.3 Ethernet / Fast Ethernet standards.

Ques 28) Discuss about the Physical Layer of Gigabit Ethernet.

Ans: Physical Layer

A mixture of technologies from the original Ethernet and ANSI X3T11 Fiber Channel Specification is used by the Physical Layer of Gigabit Ethernet. Gigabit Ethernet generally support four physical media types.

These are defined in 802.3z (1000Base-X) and 802.3ab (1000Base-T):

1) **1000Base-X:** Physical Layer of Fiber Channel is based on the 1000Base-X standard. An interconnection technology like Fiber Channel is used for connecting workstations, storage devices and peripherals. Fiber Channel has four layers architecture in which the lowest two layers FC-0 (Interface and media) and FC-1 (Encode/Decode) are used in Gigabit Ethernet. With the use of Fiber Channel, it will greatly reduce the Gigabit Ethernet standard development time.

   1000Base-X standard consists of three types of media:
   i) 1000Base-SX850 nm laser on multi mode fiber
   ii) 1000Base-LX1300 nm laser on single mode and multi-mode fiber
   iii) 1000Base-CXShort haul copper "twinax" STP cable

   Table 2.7 represents the cabling distances to be supported:

   Table 2.7: Cabling Types and Distances

Cable Type	Distance
Single-mode Fiber (9 micron)	3000m using 1300nm laser (LX)
Multi-mode Fiber (62.5 micron)	300m using 850nm laser (SX) 550m using 1300nm laser (LX)
Multi-mode Fiber (50 micron)	550m using 850nm laser (SX) 550m using 1300nm laser (LX)
Short-haul Copper	25m

2) **1000Base-T:** This is a standard for Gigabit Ethernet over long haul copper UTP. The goals of the standard committee give it the permission up to 25-100 m over 4 pairs of Category 5 UTP. Through the 802.3ab task force, this standard is being developed and is expected to be fully developed by early 1999.

WIRELESS LANS – 802.11

Ques 29) Discuss the IEEE 802.11 Standard in detail.

Or

What is Wireless LAN? And write the Wireless LAN Requirements.

Or

What is wireless LAN? What do you understand by Infrastructure and Ad-hoc Networks?

Ans: IEEE 802.11 Standards: Wireless LAN

The wireless local area network (LAN) is an alternative for a wired LAN. It is flexible data communications system implemented by way of an extension to a wired LAN. Wireless LANs transmit and receive data over the air and minimizing the need for wired connections through radio frequency (RF) technology. Therefore, wireless LANs combine data connectivity with user mobility.

The WLANs (wireless local area network) are similar to traditional LANs having a wireless interface and construing a wireless communication between the equipment connected to LAN. It may be further connected to fixed network like LAN, WAN, the internet, etc.

A main component of wireless LAN is the wireless interface card and an antenna. It can be connected to mobile unit and also to fixed network. The wireless LANs have limited range and only be in working in local geographical area such as a building, park, or office complex.

Infrastructure and Ad-hoc Networks

Wireless networks are set-up to either communicate indirectly through a central place – an access point – or directly, one to the other. The first is called **Infrastructure mode** and the other is called **ad-hoc mode** (it is also called peer-to-peer):

1) **Infrastructure Network:** Communication typically takes place only between the wireless nodes and the access point. Not directly between the wireless nodes. Access point acts as a bridge. Access points with a fixed network can connect several wireless networks to form a larger network beyond the actual radio coverage.

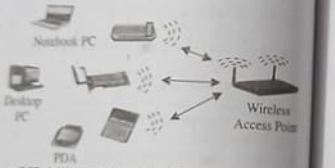


Figure 2.27: A Wireless Network in Infrastructure Mode

Infrastructure networks not only provide access to other networks, but also include forwarding functions, medium access control. Cellular phones are typically infrastructure-based networks for wide area. Also satellite-based cellular phones have an infrastructure (the satellites).

2) **Ad-Hoc Network:** A wireless ad-hoc network is a decentralized type of wireless network as shown in **figure 2.35**. The network is ad hoc because it does not rely on a pre-existing infrastructure, such as routers in wired networks or access points in managed (infrastructure) wireless networks. Instead, each node participates in routing by forwarding data for other nodes, so the determination of which nodes forward data is made dynamically on the basis of network connectivity. In addition to the classic routing, ad hoc networks can use flooding for forwarding the data. Ad hoc networks make sense when needing to build a small, all-wireless LAN quickly and spend the minimum amount of money on equipment.

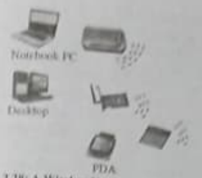


Figure 2.28: A Wireless Network in Ad-hoc Mode

Ques 30) What is the different wireless LAN Standard?

Ans: Wireless LAN Standards

The main standards of wireless LAN are:

1) **IEEE 802.11:** This standard supports 1 Mbps data rate and numerous options of physical medium such as spread spectrum and infrared. IEEE 802.11 also supports prioritized access to the medium. The extra feature of this standard is battery conservation for inactive or idle wireless users. Campus, universities and companies are encouraging for use of IEEE 802.11-based LANs.

2) **HiperLAN2:** HiperLAN2 is another emerging WLAN standard proposed by European Telecommunications Standard Institute (ETIS). It provides for use of connections that offer different quality of service for different applications and this is an exciting feature of this standard. This uses time-division multiplexing of broadcast connection, unicast and multicast connections.

3) **Bluetooth:** Bluetooth was promoted by several leaders of industry like IBM, Ericsson, Lucent, Nokia, Intel, Microsoft, Toshiba and Motorola. The Bluetooth is a wireless Personal Area Network (PAN) operating at 2.4 GHz band and offers maximum up to 1 Mbps data rate. Having low power and smaller range, Bluetooth uses frequency hopping spread spectrum (FHSS) modulation.

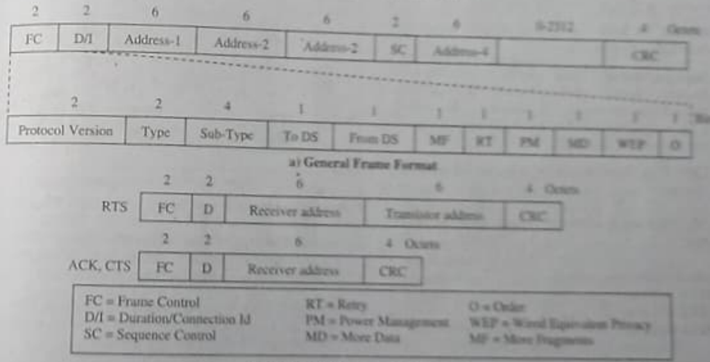
It additionally supports ad-hoc networking. **IEEE 802.11** and **HiperLAN2** are typically infrastructures based networks.

The **Bluetooth** is a wireless ad-hoc network.

Ques 31) What is the frame format of 802.11 frames?

Ans: 802.11 Frame Format

Figure 2.29(a) shows the general format of the control and data of IEEE 802.11 frames. Formats of RTS, CTS and ACK frames have reduced number of fields as shown in **figure 2.29 (b)**.



a) General Frame Format

b) Format of RTS, CTS, ACK frames

Figure 2.29: Format of IEEE 802.11 Frame

1) **Frame Control (FC, 2 octets):** It indicates the type of frame. Some of its important subfields are as under:
   i) **Protocol version (2 bits):** This field indicates the version of IEEE 802.11 protocol being used.
   ii) **Type (2 bits):** This field indicates the type of frame (control, data, management).
   iii) **Sub-type (4 bits):** This field indicates the sub-type of the frame.
   iv) **To DS (1 bit):** This bit is set to 1 if the frame is destined for DS.
   v) **From DS (1 bit):** This bit is set 1 if the frame is coming from DS.
   vi) **MF (More Fragment, 1 bit):** This bit is set to 1 if more fragments are to follow.
   vii) **RT (Retry, 1 bit):** This bit is set to 1 if this frame is retransmission of previous frame.

viii) **PM (Power management, 1 bit):** This bit is set to 1 if the transmitting station is in sleep mode.

ix) **MD (More data, 1 bit):** This bit when set 1 indicates that the transmitting station has more data to send.

x) **WEP (Wired equivalent privacy, 1 bit):** This bit is 1 if the wired equivalent privacy protocol is implemented.

xi) **Order (1 bit):** If the service provided by the MAC sublayer is 'Strictly Ordered' service, this bit is set to 1.

2) **Q/I (Duration/connection Id, 2 octets):** As duration field, it indicates the time in microseconds, the channel is reserved for reliable transmission of a MAC frame and its acknowledgement. As connection-id field, it identifies an association or a connection.

3) **Address fields (6 octets each):** There can be up to four address fields. Their number and use depend on the context. DA and SA are the destination address and source address respectively. The remaining terminology is as follows:

BSS-Id	BSS Identifier
RA	Receiver Address
TA	Transmitter Address

RA and TA refer to addresses of APs within the Distribution System (DS).

4) **Sequence control (SC, 2 octets):** It contains 4-bit fragment number subfield which is used for fragmentation and reassembly. The other 12-bit subfield is the sequence number of the frame sent between a given pair of transmitter and receiver.

5) **CRC:** It is 32-bit frame CRC sequence for detection of errors.

Ques 32) What are the different versions of IEEE 802.11 standard?

Or

Explain the following in detail:

1) IEEE 802.11a
2) IEEE 802.11b
3) IEEE 802.11g

Ans: Versions of IEEE 802.11 Standards

1) **IEEE 802.11a:** IEEE 802.11a, ratified in 1999, is the amendment to the IEEE 802.11 specification with a higher throughput upto 54Mbps.

IEEE 802.11a operates on 5GHz. As compared to other IEEE 802.11 standards, such as IEEE 802.11b/g, it has less interference, since the 2.4GHz band is heavily used. However, its penetration is also reduced, due to its higher carrier frequency, so the signals are absorbed readily by solid objects along its **propagation path.**

2) **IEEE 802.11b:** IEEE 802.11b operates on 2.4GHz band with throughput of upto 11Mbps, which was released in 1999 and was marketed under the name Wi-Fi. IEEE 802.11b uses a direct extension of Direct Sequence Spread Spectrum DSSS on the PHY layer.

3) **IEEE 802.11g:** The IEEE's 802.11g standard is a higher-bandwidth successor to the popular 802.11b, or Wi-Fi standard. 802.11g operates at a maximum speed of 54Mbps whereas 802.11b has a maximum speed of 11Mbps (Megabits/sec).

An 802.11g access point compatible with both 802.11b and 802.11g clients. As a result, a laptop computer with an 802.11g card will be able to access existing 802.11b access points as well as new 802.11g access points.

Ques 33) What are the IEEE 802.11 Architecture.

Ans: IEEE 802.11 Architecture

Figure 4.12 shows the architecture of 802.11:

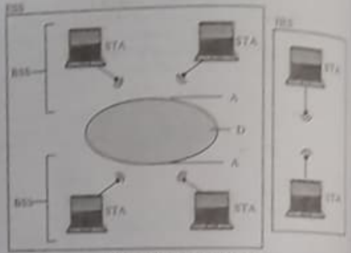


Figure 2.30: 802.11 Architecture

Following are the main components of the 802.11 logical architecture:

1) **Access Point (AP):** This is the central point which creates a basic services set to connect a number of STAs from the wireless network to other available networks.

2) **Station (STA):** A desktop computer, laptop, or PDA is a type of wireless network client and STA is the basic component of the wireless network.

Station may be considered as a device which contains the functionality of the 802.11 protocol, that being MAC PHY, and a connection to the wireless media. Basically, the 802.11 functions are implemented in the hardware and software of a network interface card (NIC).

3) **Basic Service Set (BSS):** The basic service set (BSS) is defined by IEEE 802.11 and is considered as the building block of a wireless LAN. This can be either stationary or mobile wireless stations. It can also be a central base station which is known as the access point (AP). The infrastructure mode will need minimum one AP to form a BSS.

4) **Extended Service Set (ESS):** It is a group of two or more wireless APs connected to the similar network that defined a single logical network segment bounded by a router (called as subnet).

5) **Portal:** It is considered as an Internetworking unit in other LAN.

6) **Independent Basic Service Set (IBSS):** This is wireless network and consists of at least two stations and uses no access point.

NETWORKING DEVICES

Ques 34) Explain the Bridges and Switches with example? And write the type of Bridges and Switches.

Ans: Networking Devices-Bridges and Switches

1) **Bridges:** A bridge is used to connect the roads across a river or valley, so using bridge automobiles can continue the driving from one side to another. Similarly, in computer network, bridge also solves the same purpose. Here bridges connect two or more networks (LANs). In case of computer network data travels from one network to other. Bridges also filter the traffic. It divides the LAN into segment to reduce the amount of traffic.

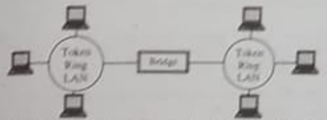


Figure 2.31: Bridges Connect Networks that use same Protocols

Types of Bridges

i) **Transparent Bridges:** Hardware network address (contains unique address) are used by the transparent bridges to identify that which data is to be passed and which to filter. A table is used to store the port information so when data is received then the stores table is used to compare against the destination address. There are four LANs networked using three bridges in a tree topology as shown in **figure 5.32**.

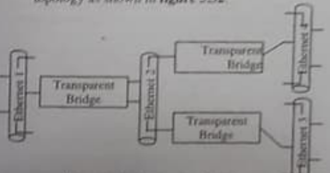


Figure 2.32: Transparent Bridge

The transparent bridge uses a *routing algorithm known as a spanning-tree algorithm*.

ii) **Source-Route Bridges:** Generally source-route bridges are used by ring networks. They do not use the MAC address for the identification while they used the token ring frame's information for the identification (whether to pass the data or not).

iii) **Translational Bridges:** To connect the dissimilar networks together, translational bridges are used. They have port for the various kinds of networks and the process used to pass the data depends on the connected networks. They consider the media access method to handle the conversation of the frame from the one type to another.

2) **Switches:** The digital switch is the heart (core) of the modern network systems which provides a transparent signal path between any pair of attached devices. This connection allows full duplex transmissions. The network interface stands for the functions and hardware required for connecting digital devices to the network. Digital switches are thus, single circuit-switching nodes.

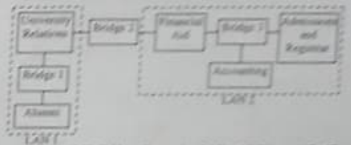


Figure 2.33: Bridges Connecting LANs with Frequent Traffic

A switch provides an answer to this problem by ensuring growth without jeopardising performance. The switch connects two or more devices on the network and allows smooth communication between nodes. Switches are executed in hardware and also software and as a result all connections operate simultaneously making the operations fast. Computers connected to a switch or hubs have no competition for bandwidth.

Types of Switches

i) **Cut-Through Switch:** A cut-through switch is inexpensive and fast. An incoming packet's address is seen by a cut-through switch and immediately sends it out to the destination LAN section. Although, if that segment is in use, a collision will occur and error recovery must be invoked.

ii) **Store-and-Forward Switch:** Each incoming packet is brought into memory by a store-and-forward switch. In this switch, it examines the destination segment and if it is busy, the switch holds the packet until the segment is free and then sends it out.Store-and-forward switches are generally slower and costly due to their memory, but buffering is the result due to the some errors on the LAN.

Ques 35) Differentiate bridges and switches? (2019, 2021[05])

Ans: Differentiate between Switches and Bridges
Table 1 shows the difference between Switches and Bridges.

Table 1: Difference between Switch and Bridge

Basis	Bridge	Switch
Basic	A bridge can connect fewer LAN.	A switch can connect more networks compared to the bridge.
Buffer	Bridges do not have buffers.	Switch has a buffer for each link connected to it.
Types	Simple bridge, multiport bridge and transparent bridge.	Store-and-forward switch and cut-through switch.
Error	Bridges do not perform error checking.	Switches perform error checking.

Ques 36) Describe bridges from 802.x to 802.y in detail.

Ans: Bridges from 802.x to 802.y
Figure 4-40 illustrates the operation of a simple two-port bridge. Host A on a wireless (802.11) LAN has a packet to send to a fixed host, B, on an (802.3) Ethernet to which the wireless LAN is connected.

The packet descends into the LLC sublayer and acquires an LLC header (black in the figure). Then it passes into the MAC sublayer and an 802.11 header is prepended to it (also a trailer).

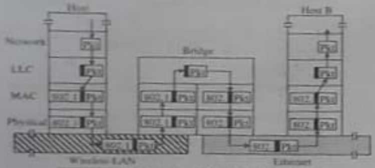


Figure 2.34: Operation of a LAN Bridge from 802.11 to

When it hits the bridge connecting the 802.11 network to the 802.3 network, it starts in the physical layer and works its way upward. In the MAC sublayer in the bridge, the 802.11 header is stripped off.

The bare packet (with LLC header) is then handed off to the LLC sublayer in the bridge. Here, the packet is destined for an 802.3 LAN, so it works its way down the 802.3 side of the bridge and off it goes on the Ethernet.

To start with, each of the LANs uses a different frame format. Unlike the differences between Ethernet, token bus, and token ring, which were due to history and big corporate egos, here the differences are to some extent legitimate. **For example,** the Duration field in 802.11 is there due to the MACAW protocol and makes no sense in Ethernet. As a result, any copying between different LANs requires reformatting, which takes CPU time, requires a new check-sum calculation, and introduces the possibility of undetected errors due to bad bits in the bridge's memory.

A **second problem** is that interconnected LANs do not necessarily run at the same data rate. When forwarding a long run of back-to-back frames from a fast LAN to a slower one, the bridge will not be able to get rid of the frames as fast as they come in.

A **third problem**, and potentially the most serious of all, is that different 802 LANs have different maximum frame lengths. Another point is security. Both 802.11 and 802.16 support encryption in the data link layer.

Ethernet does not. This means that the various encryption services available to the wireless networks are lost when traffic passes over an Ethernet.

One solution to the security problem is to do encryption in a higher layer but then the 802.11 station has to know whether it is talking to another station on an 802.11 network or not. Forcing the station to make a choice destroys transparency.

A final point is quality of service. Both 802.11 and 802.16 provide it in various forms, the former using PCF mode and the latter using constant bit rate connections.

Ethernet has no concept of quality of service, so traffic from either of the others will lose its quality of service when passing over an Ethernet.

Ques 37) Explain the following devices in details:
1) Repeaters
2) Hub

Or

What is repeater? Discuss its types also.

Or

What is the role of hub in networking? Discuss about its types.

Or

What is active and passive hub? Describe.

Ans:

1) **Repeaters:** Repeaters are used to connect the two or more than two similar LAN networks. Over wire it also extends the reach. While two or more networks are connected using same protocol it repeats the signals.

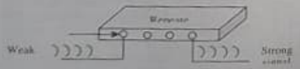


Figure 2.35: Repeater Regenerates a Weak Signal

A repeater is a device which receives a digital signal on a transmission medium and regenerates the signal across the next medium. The repeaters reduce the attenuation caused by free-space electromagnetic-field divergence or cable loss. A sequence of repeaters makes possible the extension of a signal over a long distance.

Types of Repeaters
Following are the types of repeaters:

i) **Single Port Repeater:** It operates with the following segments:
   a) In first part the signal is taken from the source and transferred to a multiport repeater.
   b) In this, one segment is connected with the other cable segment.

ii) **Multiport Repeater:** It has multiple output port and single input port.

iii) **Smart Repeater:** It is a hybrid repeater device. Its functionality is similar to a bridge. Smart repeaters are used for the packet filtering.

iv) **Optical Repeater:** In all types of cable, these repeaters can implement. They repeat the optical signals.

2) **Hub:** Hubs act as central attachment point for network cables and hence are network connectivity devices which are positioned centrally.

These are available for all guided media barring Ethernet cable. Star topology refers to the topology of a network which uses hub. Hubs can connect multiple communication devices as it has multiple ports.

Adding or removing a device is fairly simple in hubs. Any cable break can also be easily detected.

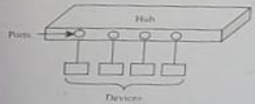


Figure 2.36: A Hub

Types of Hub
There are three categories of hubs i.e., passive, active and intelligent hub:

i) **Active Hub:** They have electronic components which can amplify and clean-up signals. The whole process is referred to as signal regeneration as the original signals are regenerated by cleaning the deformed elements.

Thus, the network becomes stronger and the distance between devices can be amplified. Active hub is similar to passive hub but it can perform the extra task.

ii) **Passive Hub:** These do not have any electronic components and thus do not process any data signal. They only combine the signals from many attached devices on the network who receive the data packets that move through the hub.

The purpose of the Passive hubs is to combining signals from different network cable sections. They are not made of any type of electronic component and data signals are not carried out for processing.

Data packets are transferred through the hub when all devices connected to the passive hub transfer data packets.

iii) **Intelligent Hub:** Enhanced active hubs are called intelligent hubs which are designed for network administrative work.

Network management protocol enables hubs to send packets to central network console which in turn can control the hubs.

For example, the network administrator might command shut down of a connection (which is generating network errors).

Ques 38) Describe about the router and gateways in detail.

Or

What are the different types of routers? What are the advantages and disadvantages of routers?

Ans: Router and Gateways

1) **Routers:** Routers are used to route the data packets along networks and connected minimum two networks.

   For example, consider the following group of networks:
   i) LANs or WAN
   ii) LAN and its ISPs

   Routers are used where gateways are placed.

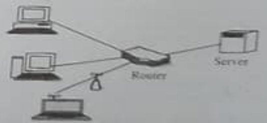


Figure 2.37: Router

Types of Router
Following are the two basic types of routers:

i) **Static Router:** In the static router, routing table is manually configured (specify the every route).

ii) **Dynamic Router:** In this, the first route is manually configured and all other routes & networks are automatically discovered.

On the basis of the cost and amount of link traffic it selects the best routes. It has the ability to direct the packets over the alternate routers.

2) **Gateways:** According to different network protocols, if two networks operate then a gateway is used to connect them. Network gateways can operate at any level of the OSI model on the basis of the types of protocols.

Gateways typically work on OSI layer 4 or higher and basically translate protocols to allow terminals to be communicated over two separate networks.

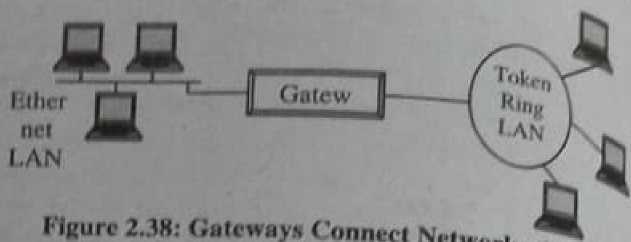


Figure 2.38: Gateways Connect Networks that use

This may be an either combinations of hardware software. The can be implemented by usin specialized software or by specially designed circu card in a standard PC. **For example,** an Interne service provider (ISP) is a gateway which connect users in a home to the Internet. The gateway is al referred to a computer routing traffic in a organization from individual workstations to a outside network's Web server. Due to the protoco translation, they may undergo from slow performance