DATA COMMUNICATION AND NETWORKS

Mrs. M. PITCHAMMAL

1. Introduction and Physical Layer

1.1Introduction

In today's world, the communication is deciding the all facts of the growth. Effective, easiest, understandable, timely communications are creating the world's better growth. The growth of the internet, telecommunication field, communication devices make the people interactive, happily and wealthy. An event happens in place can be communicated to any place in the world. For example, a live sports event happened in Calcutta can be viewed by the people sitting in any place in the world.

The network allows people to communicate information to any people in the world by means of one-to-one, one-to-many or all. In this chapter, we are going to study about the introduction of networks, network hardware, network software and network architecture.

Data Communication

- Data

  The word 'data' refers that representation of information in an understandable form by the two parties who are creating and using it. The Webster dictionary defined data as "*information in digital form that can be transmitted or processed*". The data may be in any form such as text, symbols, images, videos, signals and so on.

- Communication

  Communication is a referred as exchanging information from one entity to another entity in a meaningful way. The entities may be referred as human being, machines, animals, birds, etc. The communication could be done between the two entities / parties.

- Data Communication

  "*Data communication is process of exchanging data between two devices through a communication medium in a meaningful way*". the four fundamental characteristics must be followed;

  1. Delivery : The data to be communicated must be delivered to the correct destination.
  2. Accuracy : The data should be delivered accurately as it is without any alteration.

3. Timeliness : The communication system must deliver the data without any delay.
4. Jitter : In network the data are split into smaller groups (packets) and send them separately. The variation of the arrival between two packets is referred as jitter.

Components

The following five components are the essential part of the communication system and figure components of data communication shows the representation of the components placement in the communication system.

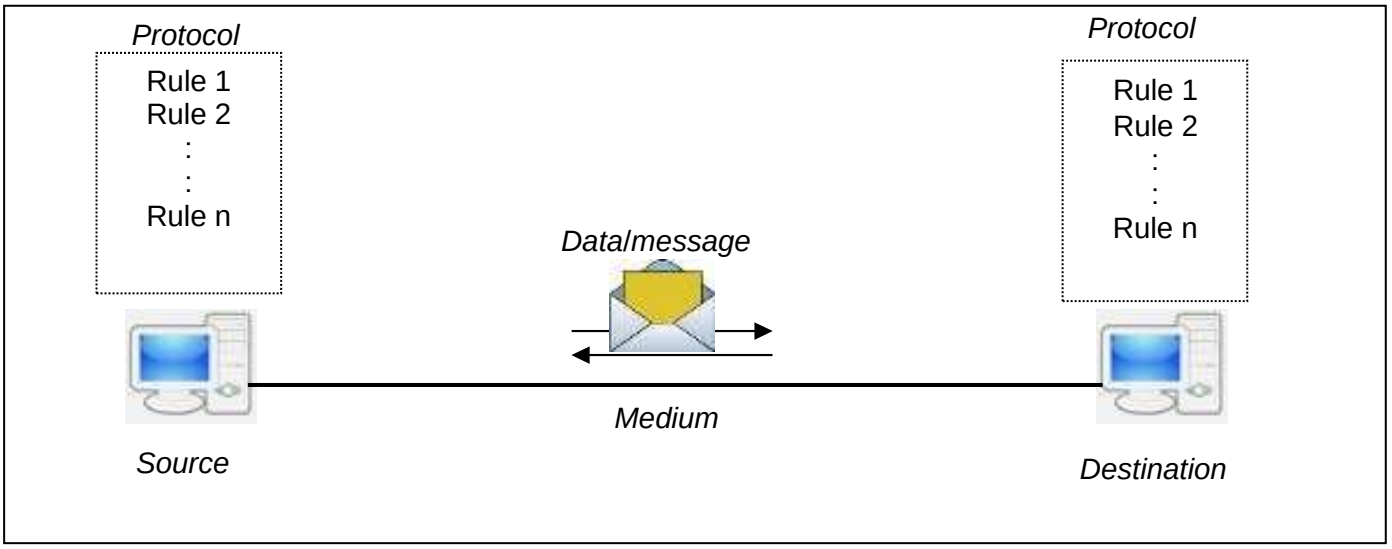


Fig Components of Data Communication

5. Data/Message : It is the primary part of the communication system. The information is communicated between the source and destination is called data/ messages
6. Source : The source is a device which generates and sends the data to the destination.
7. Destination : It is a device that receives the data.
8. Medium : It acts as carrier to carry the data from the source to the destination. The carrier provides the path through wire or wireless.
9. Protocol : It is set of rules that govern the data communication in a correct manner.

The source and destination may be computer, mobile phones, workstations, servers, video cameras and so on. The protocol provides the effective communication. This provides the methodology how to interact with each other without any loss or interference.

Mode of Data Flow

The data flow defines the flow direction of the data between source and destination. The data flow may be either simplex or half-duplex or full duplex. The figure data flow shows the three modes of the data flow.

Communication between two devices can be of three types. They are

1. **Simplex:** The communication is unidirectional. Only one of the two stations on a link can transmit and other can only receive
2. **Half duplex:** Each station can both transmit and receive but not at the same time.
3. **Full-duplex:** Both station can both transmit and receive data at the same time.

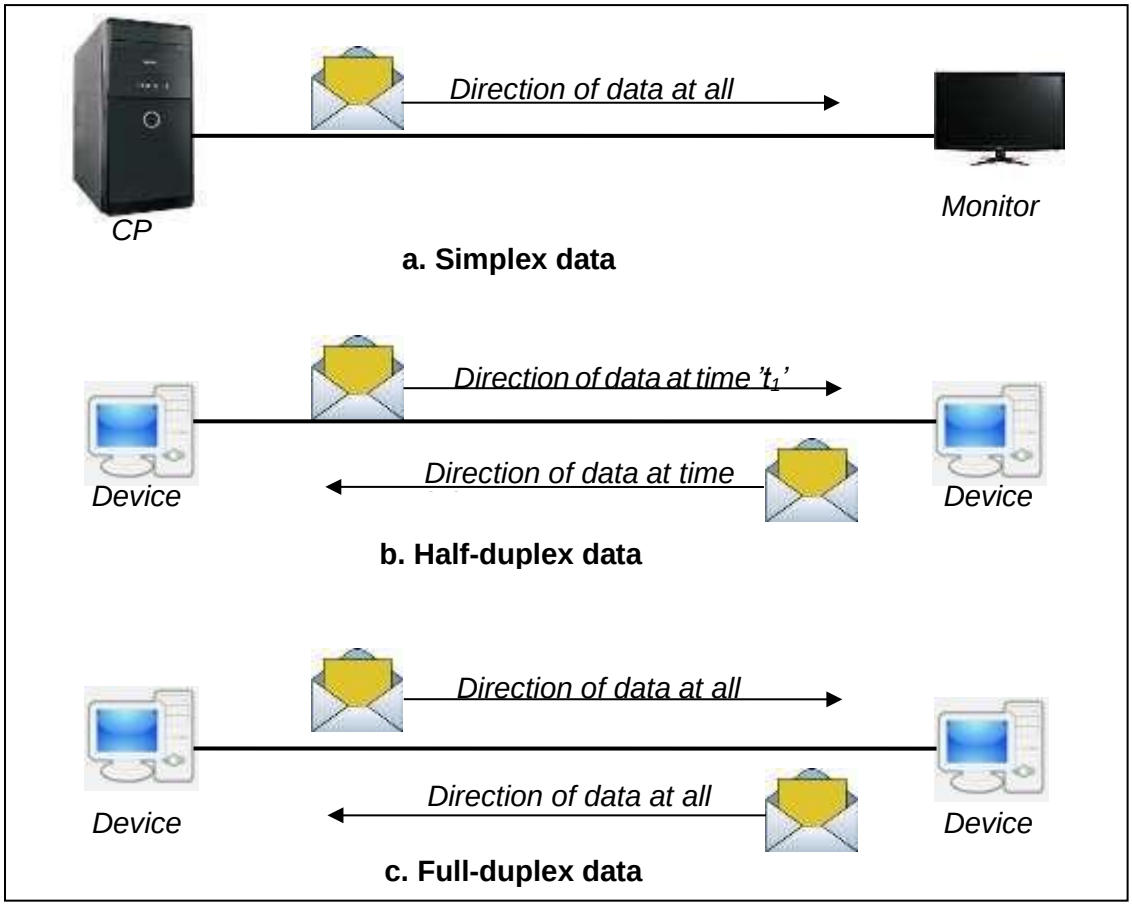


Fig: data flow mode

1.1.1Networks

A network is set of interconnected devices (sometime referred as nodes) which are used to transmit data between them with agreed protocols. The networks are used to connect the people, machines, devices to share the data anywhere in the world. The devices can be computers, printers, mobile phones, servers which are capable of sending and receiving data. The data can be generated by a device.

History of Network

A computer network is a digital telecommunications network which allows nodes

to share resources. In computer networks, computing devices exchange data with each other using connections (data links) between nodes. These data links are established over cable media such as wires or optic cables, or wireless media such as Wi-Fi.

Computer networking as we know it today may be said to have gotten its start with the Arpanet development in the late 1960s and early 1970s. Prior to that time there were computer vendor "networks" designed primarily to connect terminals and remote job entry stations to a mainframe.

In 1940, George Sitbit used a teletype machine to send instructions for a problem set from his model at Dartmouth college to his complex number calculator in New York and received results back by the same means. In 1950's, early networks of communicating computers included the military radar system Semi-Automatic Ground Environment (SAGE) was started.

Later, in 1960s, the notion of networking between computers viewing each other as equal peers to achieve "resource sharing" was fundamental to the ARPAnet design [1]. The other strong emphasis of the Arpanet work was its reliance on the then novel technique of packet switching to efficiently share communication resources among "bursty" users, instead of the more traditional message or circuit switching. The table 1.1 gives the time frame of the computer network growth from network to internet.

Year	**Event**
1961	The idea of ARPANET, one of the earliest computer networks, was proposed by Leonard Kleinrock in 1961, in his paper titled "Information Flow in Large Communication Nets."
1965	The term "packet" was coined by Donald Davies in 1965, to describe data sent between computers over a network.
1969	ARPANET was one of the first computer networks to use packet switching. Development of ARPANET started in 1966, and the first two nodes, UCLA and SRI (Standford Research Institute), were connected, officially starting ARPANET in 1969.
1969	The first RFC surfaced in April 1969, as a document to define and provide information about computer communications, network protocols, and procedures.
1969	The first network switch and IMP (Interface Message Processor) was sent to UCLA on August 29, 1969. It was used to send the first data transmission on ARPANET.
1969	The Internet was officially born, with the first data transmission being sent between UCLA and SRI on October 29, 1969, at 10:30 p.m.
1970	Steve Crocker and a team at UCLA released NCP (NetWare Core Protocol) in 1970. NCP is a file sharing protocol for use with NetWare.
1971	Ray Tomlinson sent the first e-mail in 1971.
1971	ALOHAnet, a UHF wireless packet network, is used in Hawaii to connect the islands together. Although it is not Wi-Fi, it helps lay the foundation for Wi-Fi.

1973	Ethernet is developed by Robert Metcalfe in 1973 while working at Xerox PARC.
1973	The first international network connection, called SATNET, is deployed in 1973 by ARPA.
1973	An experimental VoIP call was made in 1973, officially introducing VoIP technology and capabilities. However, the first software allowing users to make VoIP calls was not available until 1995.
1974	The first routers were used at Xerox in 1974. However, these first routers were not considered true IP routers.
1976	Ginny Strazisar developed the first true IP router, originally called a gateway, in 1976.
1978	Bob Kahn invented the TCP/IP protocol for networks and developed it, with help from Vint Cerf, in 1978.
1981	Internet protocol version 4, or IPv4, was officially defined in RFC 791 in 1981. IPv4 was the first major version of the Internet protocol.
1981	BITNET was created in 1981 as a network between IBM mainframe systems in the United States.
1981	CSNET (Computer Science Network) was developed by the U.S. National Science Foundation in 1981.
1983	ARPANET finished the transition to using TCP/IP in 1983.
1983	Paul Mockapetris and Jon Postel implement the first DNS in 1983.
1986	The NSFNET (National Science Foundation Network) came online in 1986. It was a backbone for ARPANET, before eventually replacing ARPANET in the early 1990's.
1986	BITNET II was created in 1986 to address bandwidth issues with the original BITNET.
1988	The first T1 backbone was added to ARPANET in 1988.

1988	WaveLAN network technology, the official precursor to Wi-Fi, was introduced to the market by AT&T, Lucent, and NCR in 1988.
1988	Details about network firewall technology was first published in 1988. The published paper discussed the first firewall, called a packet filter firewall, that was developed by Digital Equipment Corporation the same year.
1990	Kalpana, a U.S. network hardware company, developed and introduced the first network switch in 1990.
1996	IPv6 was introduced in 1996 as an improvement over IPv4, including a wider range of IP addresses, improved routing, and embedded encryption.
1997	The first version of the 802.11 standard for Wi-Fi is introduced in June 1997, providing transmission speeds up to 2 Mbps.
1999	The 802.11a standard for Wi-Fi was made official in 1999, designed to use the 5 GHz band and provide transmission speeds up to 25 Mbps.
1999	802.11b devices were available to the public starting mid-1999, providing transmission speeds up to 11 Mbps.
1999	The WEP encryption protocol for Wi-Fi is introduced in September 1999, for use with 802.11b.
2003	802.11g devices were available to the public starting in January 2003, providing transmission speeds up to 20 Mbps.
2003	The WPA encryption protocol for Wi-Fi is introduced in 2003, for use with 802.11g.
2003	The WPA2 encryption protocol is introduced in 2004, as an improvement over and replacement for

	WPA. All Wi-Fi devices are required to be WPA2 certified by 2006.
2009	The 802.11n standard for Wi-Fi was made official in 2009. It provides higher transfer speeds over 802.11a and 802.11g, and it can operate on the 2.4 GHz and 5 GHz bandwidths.
2018	The Wi-Fi Alliance introduced WPA3 encryption for Wi-Fi in January 2018, which includes security enhancements over WPA2.

Table 1.1 Time period of Network growth

1.1.2Uses of Computer Networks

The computer networks are used in different applications to meet the requirement of different people at different places in different time. The following are the uses of computer network.

1. Business Applications.

Many companies have a substantial number of computers.

- **Resource sharing**: The main task of the connectivity of resources is resource sharing. For example, a high-volume networked printer may be installed instead of large collection of individual printers.
- **Information Sharing** : large and medium-sized company and many small companies are vitally dependent on computerized information.

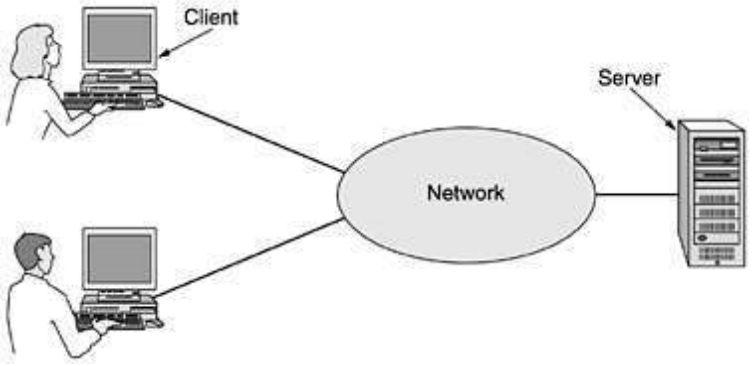


Figure : A network with two clients and one server

In client-server model in detail, two processes are involved, one on the client machine and one on the server machine. Communication takes the form of the client process sending a message over the network to the server process. The client process then waits for a reply message. When the server process gets the request, it performs the requested work or looks up the requested data and sends back a reply.

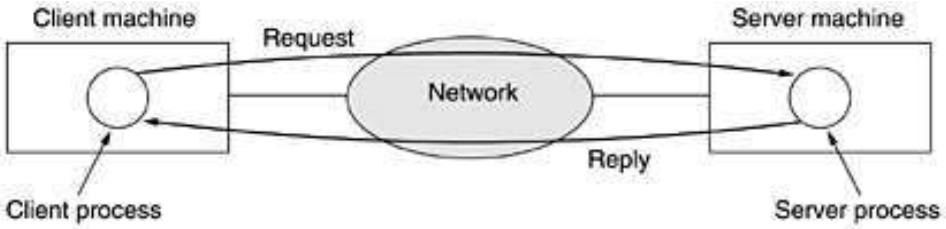


Figure :Client-server model involves requests and replies

- **Connecting People** : another use of setting up a computer network has to do with people rather than information or even computers. It is achieved through Email, Video Conferencing.
- **E-commerce** : many companies is doing business electronically with other companies, especially suppliers and customers, and doing business with consumers over the Internet.

2. Home Applications

The computer network provides better connectivity for home applications via desktop computers, laptops, iPads, iPhones. Some of the more popular uses of the Internet for home users are as follows:

- Access to remote information.
- Person-to-person communication (peer-to-peer).
- Peer-to-peer - there are no fixed clients and servers.
- Audio and Video sharing
- Interactive entertainment.
- Electronic commerce.

Tag	Full name	Example
B2C	Business-to-consumer	Ordering books on-line
B2B	Business-to-business	Car manufacturer ordering tires from supplier
G2C	Government-to-consumer	Government distributing tax forms electronically
C2C	Consumer-to-consumer	Auctioning second-hand products on line
P2P	Peer-to-peer	File sharing

Table 1.2 Some forms of e-commerce

3. Mobile Users

As wireless technology becomes more widespread, numerous other applications are likely to emerge. Wireless networks are of great value to fleets of trucks, taxis,

delivery vehicles, and repairpersons for keeping in contact with home. Wireless networks are also important to the military.

Although wireless networking and mobile computing are often related, they are not identical, as Table 1.3 shows. Here we see a distinction between fixed wireless and mobile wireless. Even notebook computers are sometimes wired. For example, if a traveller plugs a notebook computer into the telephone jack in a hotel room, he has mobility without a wireless network.

Wireless	Mobile	Applications
No	No	Desktop computers in offices
No	Yes	A notebook computer used in a hotel room
Yes	No	Networks in older, unwired buildings
Yes	Yes	Portable office; PDA for store inventory

Table 1.3 Combinations of wireless networks and mobile computing

Another area in which wireless could save money is utility meter reading. If electricity, gas, water, and other meters in people's homes were to report usage over a wireless network, there would be no need to send out meter readers.

4. Social issues

The widespread introduction of networking has introduced new social, ethical, and political problems. A popular feature of many networks are newsgroups or bulletin boards whereby people can exchange messages with like-minded individuals. As long as the subjects are restricted to technical topics or hobbies like gardening, not too many problems will arise.

The following are the issues in society due to the misbehave or misconduct of computer networks.

- Network neutrality
- Digital Millennium Copyright Act
- Profiling users
- Phishing

1.1.3Criteria of Network

A network must have the following important criteria for effective communication.

- Performance

The performance of a network is measured by many factors such as transit time, response time. The transit time is amount of time required to travel a message from source to destination. The response time is amount of time required for inquiry

and response.

- Throughput and Delay

The throughput of the network is measures as amount of data transferred for specified period of time. The high transmission within the specified period of time is called as high throughput network. The delay is measured as time difference between the transit time and actual time taken to transmit. A good network maintains high through and low delay.

- Reliability

The reliability of a network is referred as data delivery should be accurate, less frequency of break in medium, fast recovery of the physical and logical (data) errors.

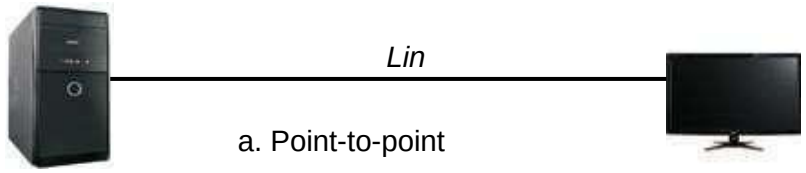
- Security

The security of a network is referred as protecting the data from damages and alteration, unauthorized access of medium, devices and data, providing mechanisms for losses and intrusions.

Types of connection

As we have already known that a network is a two or more devices interconnected through a communication medium. The medium provides the physical pathway between two devices. The connectivity between the devices is classified into point-to-point and multipoint.

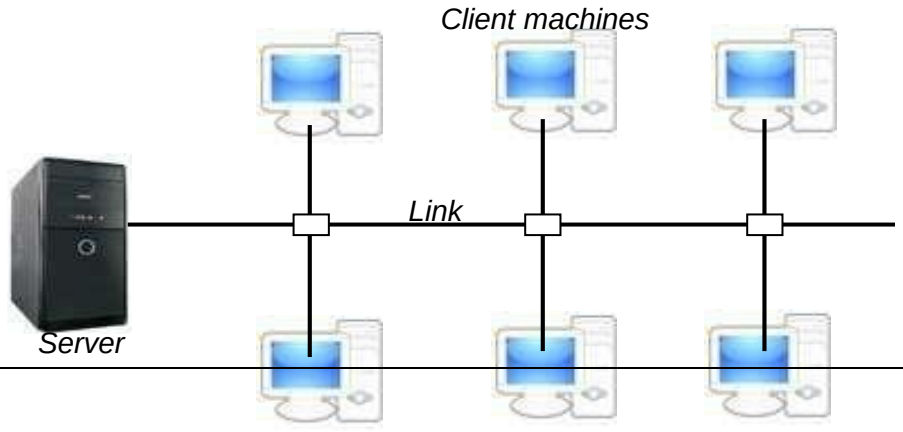
1. point-to-point
    a. It provides a direct and dedicated link between two devices (normally source and destination). The entire transmission capacity of the link is shared for these two devices only
    b. For example, link between monitor and computer.



a. Point-to-point

2. Multipoint

A link is shared by many devices and the transmission capacity is shared by



all devices connected (fig 1.6.b). For example, a cable TV network or client-server network.

b. Multipoint connection

1.2 Network Hardware

Introduction

It is now time to turn our attention from the applications and social aspects of networking (the dessert) to the technical issues involved in network design (the spinach). There are two types of transmission technology that are in widespread use: **broadcast links** and **point-to-point links**.

Point-to-point links:

Point-to-point links connect individual pairs of machines.

packets : To go from the source to the destination on a network made up of point-to-point links, short messages, called packets**.**

Unicasting: Transmission with exactly one sender and exactly one receiver is sometimes called unicasting.

Broadcast links:

On a broadcast network, the communication channel is shared by all the machines on the network; packets sent by any machine are received by all the others. An address field within each packet specifies the intended recipient.

Upon receiving a packet, a machine checks the address field. If the packet is intended for the receiving machine, that machine processes the packet; if the packet is intended for some other machine, it is just ignored.

A wireless network is a common example of a broadcast link, with communication shared over a coverage region that depends on the wireless channel and the transmitting machine

- **Broadcasting:** Broadcast systems usually also allow the possibility of addressing a packet to all destinations by using a special code in the address field. When a packet with this code is transmitted, it is received and processed by every machine on the network. This mode of operation is called broadcasting.
- **Multicasting:** Some broadcast systems also support transmission to a subset of the machines, which known as multicasting.

An alternative criterion for classifying networks is by scale. Distance is important as a classification metric because different technologies are used at different scales.

Interprocessor distance	Processors located in same	Example
1 m	Square meter	Personal area network
10 m	Room	Local area network
100 m	Building	
1 km	Campus	
10 km	City	Metropolitan area network
100 km	Country	Wide area network
1000 km	Continent	
10,000 km	Planet	The Internet

Figure: Classification of interconnected processors by scale.

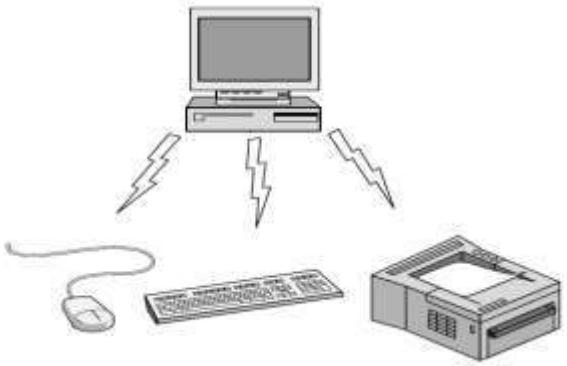
In the above Figure we classify multiple processor systems by their rough physical size. At the top are the personal area networks, networks that are meant for one person. Beyond these come longer-range networks. These can be divided into local, metropolitan, and wide area networks, each with increasing scale. Finally, the connection of two or more networks is called an internetwork. The worldwide Internet is certainly the best-known (but not the only) example of an internetwork.

1.2.1Types of Network

1. Personal Area Networks

PAN (Personal Area Networks) let devices communicate over the range of a person. It is smallest network which is very personal to a user. PAN has connectivity range up to 10 meters.

A common example is a wireless network that connects a computer with its peripherals. Almost every computer has an attached monitor, keyboard, mouse, and printer. This may include Bluetooth enabled devices or infra-red enabled devices.

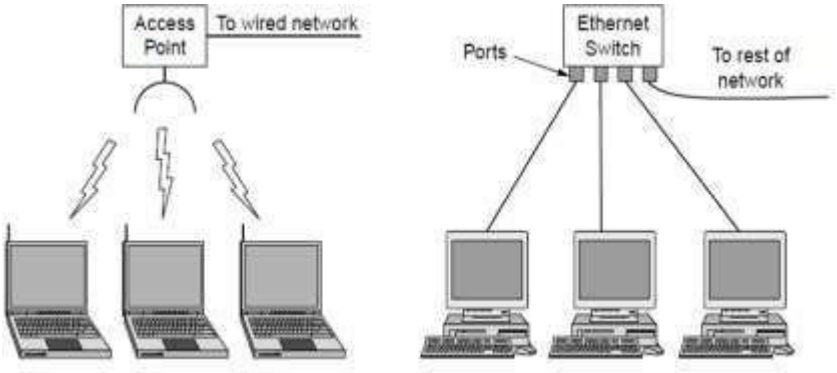


2. LAN (Local Area Network)

It is normally private and will connect computer in a small area such as the entire

computer in single company or building. The network at your business or school is an example of a LAN.

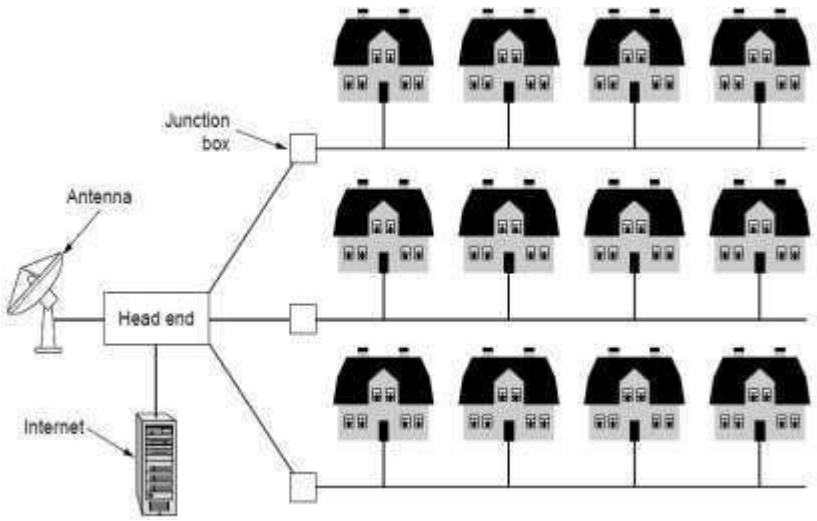
Early LENs had data rates in the 4 to 16 megabits per second (Mbps) range. Today, however, speeds are normally 100 or 1000 Mbps.



3. MAN (Metropolitan Area Network)

It is a "LAN" that has been extended so that it covers a larger area such as an entire city.

The best-known examples of MANS are the cable television networks available in many cities. These systems grew from earlier community antenna systems used in areas with poor over-the-air television reception. In those early systems, a large antenna was placed on top of a nearby hill and a signal was then pipe to the subscribers houses.



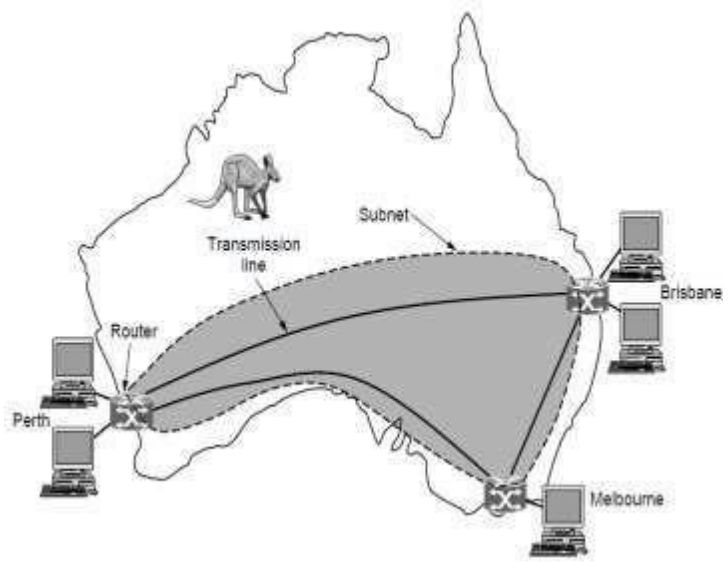
4.Wide Area Networks

A wide area network (WAN) provides long-distance transmission of data, image, audio and video information over large geographic areas that may comprise a country, a continent, or even the whole world

In most WAN's the subnet consist of two distinct components:

1. Transmission lines

2 Switching elements.



1. Transmission lines

Transmission lines move bits between machines. They can be made of copper wire, optical fiber, or even radio links. Most companies do not have transmission lines lying about. so instead they lease the lines from a telecommunications company.

2. Switching elements

Switching elements, or just switches, are specialized computers that connect two or more transmission lines. When data arrive on an incoming line, the switching element must choose an outgoing line on which to forward them.

3. Router These switching computers have been called by various names in the past; the name **router** is now most commonly used.

5.Internetworks

People connected to one network often want to communicate with people attached to a different one. The fulfillment of this desire requires that different, and frequently incompatible, networks be connected. A collection of interconnected networks is called an **internetwork** or **internet**.

Subnets, networks, and internetworks are often confused. The term ‘‘subnet’’ makes the most sense in the context of a wide area network, where it refers to the collection of routers and communication lines owned by the network operator. A network is formed by the combination of a subnet and its hosts. A subnet might be described as a network, as in the case of the ‘‘ISP network’’ of Figure 1.12 An internetwork might also be described as a network, as in the case of the WAN in Figure 1.10

- **Gateway:** The general name for a machine that makes a connection between two

or more networks and provides the necessary translation, both in terms of hardware and software, is a **gateway**. Gateways are distinguished by the layer at which they operate in the protocol hierarchy.

Since the benefit of forming an internet is to connect computers across networks, we do not want to use too low-level a gateway or we will be unable to make connections between different kinds of networks. We do not want to use too high-level a gateway either, or the connection will only work for particular applications.

The level in the middle that is ‘‘just right’’ is often called the network layer, and a router is a gateway that switches packets at the network layer. We can now spot an internet by finding a network that has routers.

1.3Network Software

Computer hardware was the main concern at the starting of computer development. Later the network software is highly required. In the following sections we examine the software structuring technique in some detail.

1.3.1Protocol Hierarchies

To reduce their design complexity, most networks are organized as a stack of layers or levels, each one built upon the one below it. The number of layers, the name of each layer, the contents of each layer, and the function of each layer differ from network to network. The purpose of each layer is to offer certain services to the higher layers, shielding those layers from the details of how the offered services are actually implemented.

Layer *n* on one machine carries on a conversation with layer n on another machine. The rules and conventions used in this conversation are collectively known as the layer *n* protocol. A five-layer network is illustrated in Fig. 1-13. The entities comprising the corresponding layers on different machines are called peers. The peers may be processes, hardware devices, or even human beings. In other words, it is the peers that communicate by using the protocol.

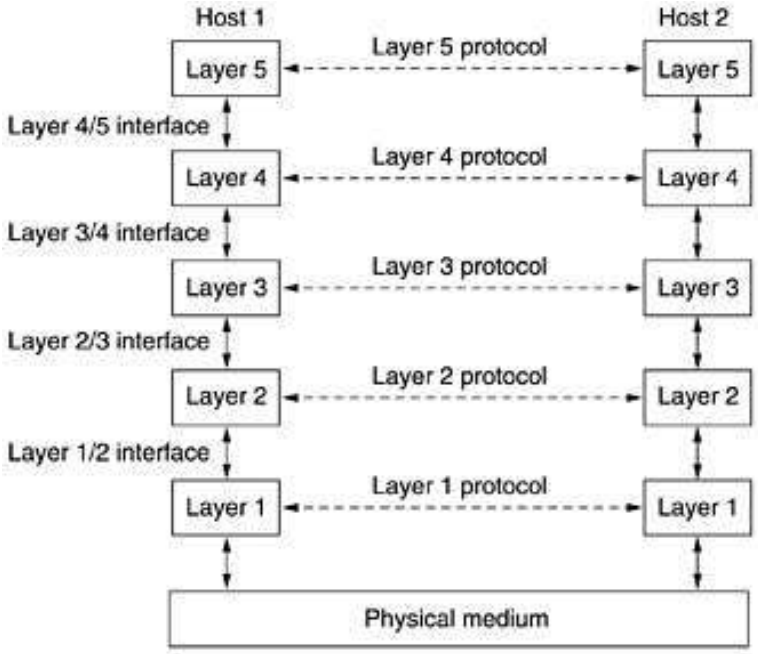


Figure : Layers, protocols, and interfaces

In reality, no data are directly transferred from layer n on one machine to layer n on another machine. Instead, each layer passes data and control information to the layer immediately below it, until the lowest layer is reached. Below layer 1 is the physical medium through which actual communication occurs. In the above figure virtual communication is shown by dotted lines and physical communication by solid lines between each pair of adjacent layers is an interface.

The interface defines which primitive operations and services the lower layer makes available to the upper one. A set of layers and protocols is called a ***network architecture***. List of protocols used by a certain system, one protocol per layer, is called a ***protocol stack***.

1.3.2 Design Issues for the Layers

Some of the key design issues that occur in computer networks are present in several layers. The following are briefly mention some of the more important ones.

- ***Identifying senders and receivers*** - some form of addressing is needed in order to specify a specific source and destination.
- ***Rules for data transfer*** - The protocol must also determine the direction of data flow, how many logical channels the connection corresponds to and what their priorities are. Many networks provide at least two logical channels per connection, one for normal data and one for urgent data.
- ***Error control*** – when circuits are not perfect, both ends of the connection must agree on which error-detecting and error-correcting codes is being used.
- ***Sequencing*** - protocol must make explicit provision for the receiver to allow the

pieces to be reassembled properly.

- ***Flow Control*** - how to keep a fast sender from swamping a slow receiver with data. This is done by feedback-based (receiver to sender) or agreed-on transmission rate.
- ***Segmentation and reassembly*** - several levels are the inability of all processes to accept arbitrarily long messages. It leads to mechanisms for disassembling, transmitting, and then reassembling messages.
- ***Multiplexing and demultiplexing*** – to share the communication medium by several users.
- ***Routing*** - When there are multiple paths between source and destination, a route must be chosen.

1.3.3 Connection-Oriented and Connectionless Services

Connection-oriented : the service user first establishes a connection, uses the connection, and then releases the connection. During the connection establishment, some negotiation is carried out about parameters to be used, such as maximum message size, quality of service required, and other issues. For example, it is looks like a telephone conversation.

Connectionless : the service user sends data when it is ready without checking anything. Each message carries the full destination address, and each one is routed through the system independent of all the others.

Here, summarizes the types of services used for connection-oriented or connectionless services for different purposes.

	Service	Example
Connection-oriented	Reliable message stream	Sequence of pages
	Reliable byte stream	Remote login
	Unreliable connection	Digitized voice
Connection-less	Unreliable datagram	Electronic junk mail
	Acknowledged datagram	Registered mail
	Request-reply	Database query

1.3.4 Service Primitives

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. 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.

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

1.3.5 Network Architecture

Protocols

A protocol is a set of rules that govern data communications. A protocol defines what is communicated, how it is communicated, and when it is communicated. The key elements of a protocol are syntax, semantics, and timing.

- **Syntax.** The term *syntax* refers to the structure or format of the data, meaning the order in which they are presented. For example, a simple protocol might expect the first 8 bits of data to be the address of the sender, the second 8 bits to be the address of the receiver, and the rest of the stream to be the message itself.
- **Semantics.** The word *semantics* refers to the meaning of each section of bits. How is a particular pattern to be interpreted, and what action is to be taken based on that interpretation? For example, does an address identify the route to be taken or the final destination of the message?
- **Timing.** The term *timing* refers to two characteristics: when data should be sent and how fast they can be sent. For example, if a sender produces data at 100 Mbps but the receiver can process data at only 1 Mbps, the transmission will overload the receiver and some data will be lost.

The two most **widely referenced protocol architectures** that served as the basis for the development of interoperable communications standards are

[1]. OSI architecture or OSI reference model and

[2]. Internet architecture or TCPIP protocol suite

TCPIP is the most widely used interoperable architecture and OSI has become the standard model for classifying communications functions.

1.3.6 OSI Reference Model

An ISO standard that covers all aspects of network communications is the Open Systems Interconnection model. It was first introduced in the late 1970s. An open system is a set of protocols that allows any two different systems to communicate regardless of their underlying architecture.

The purpose of the OSI model is to show how to facilitate communication between different systems without requiring changes to the logic of the underlying hardware and software. The OSI model is not a protocol; it is a model for understanding and designing a network architecture that is flexible, robust, and interoperable.

ISO is the organization. OSI is the model.

The OSI model is composed of seven ordered layers:

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

It consists of seven separate but related layers, each of which defines a part of the process of moving information across a network the layers involved when a message is sent from device A to device B. As the message travels from A to B, it may pass through many intermediate nodes. These intermediate nodes usually involve only the first three layers of the OSI model.

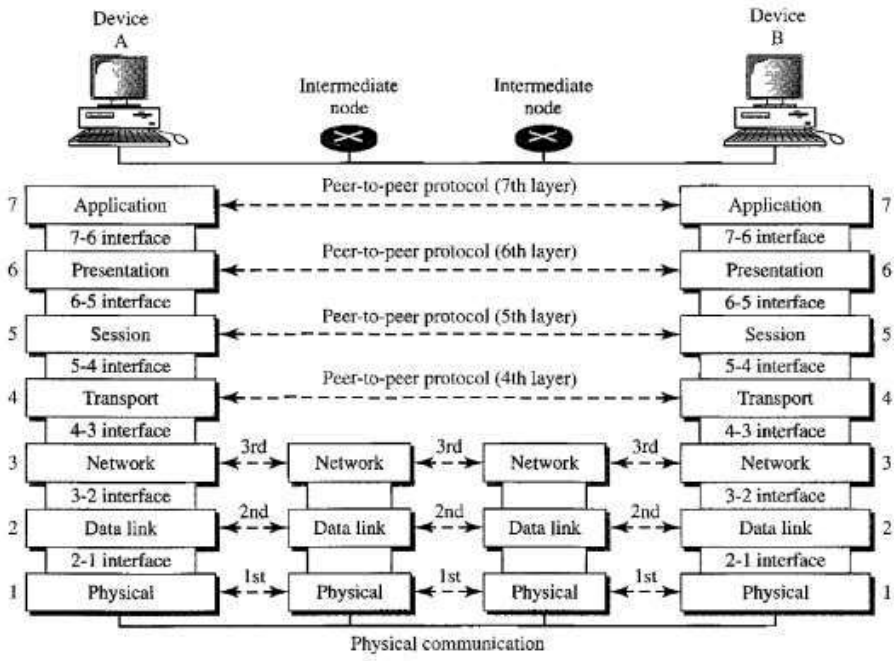
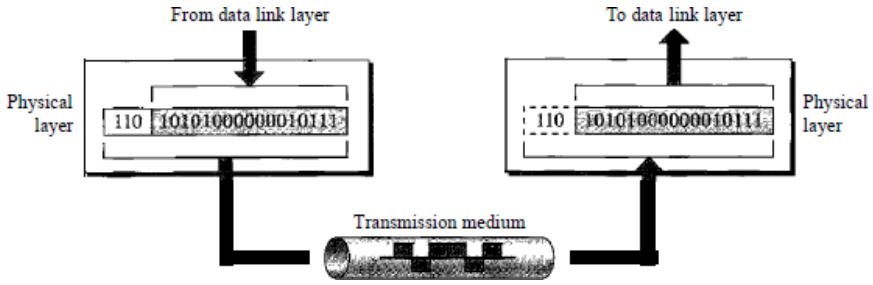


Figure: The interaction between layers in the OSI model

Within a single machine, each layer calls upon the services of the layer just below it. Layer 3, for example, uses the services provided by layer 2 and provides services for layer 4. Between machines, layer *x* on one machine communicates with layer *x* on another machine. This communication is governed by an agreed-upon series of rules and conventions called protocols. The processes on each machine that communicate at a given layer are called peer-to-peer processes. Communication between machines is therefore a peer-to-peer process using the protocols appropriate to a given layer.

1.Physical layer

The physical layer coordinates the functions required to transmit a bit stream over a physical medium. It deals with the mechanical and electrical specifications of the interface and the transmission medium. The functions are,



a. Physical Characteristics of Interfaces and Media

It defines the electrical and mechanical characteristics of the interface and the media. It defines the types of transmission medium.

b. Representation of Bits

To transmit the stream of bits they must be encoded into signal. It defines the type of encoding weather electrical or optical.

C. Data Rate

It defines the transmission rate to the number of bits sent per second.

d. Synchronization of Bits

The sender and receiver must be synchronized at bit level

e. Line Configuration

It defines the type of connection between the devices. Two types of connection are

a) point to point b) multipoint

f. Physical Topology

It defines how devices are connected to make a network. Five topologies are mesh, star, tree, bus, and ring.

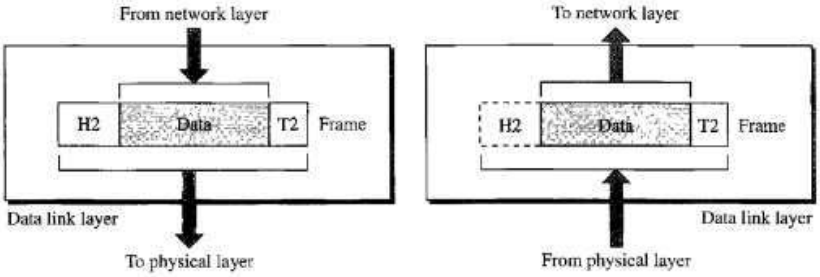
g. Transmission Mode

It defines the direction of transmission between devices Three types of transmission are

Simplex, half duplex, full duplex

2.Data Link Layer

Data Link layer is responsible for node-to-node delivery. The responsibilities of Data Link layer are,



a. Framing

It divides the stream of bits received from network layer into manageable data units called frames **. b.Physical Addressing**

It adds a header that defines the physical address of the sender and the receiver. If the sender and the receiver are in different networks, then the receiver address is the address of the device which connects the two networks.

c. Flow Control

It imposes a flow control mechanism used to ensure the data rate at the sender and the receiver should be same.

d. Error Control

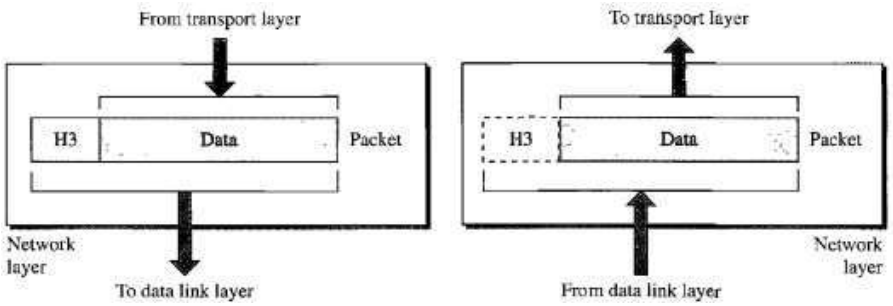
To improve the reliability the Data Link layer adds a trailer which contains the error control mechanism like CRC, Checksum etc.

e. Access Control

When two or more devices connected at the same link, then the Data Link layer used to determine which device has control over the link at any given time

3.Network Layer

When the sender is in one network and the receiver is in some other network then the network layer has the responsibility for the source to destination delivery. The responsibilities are,



a. Logical Addressing

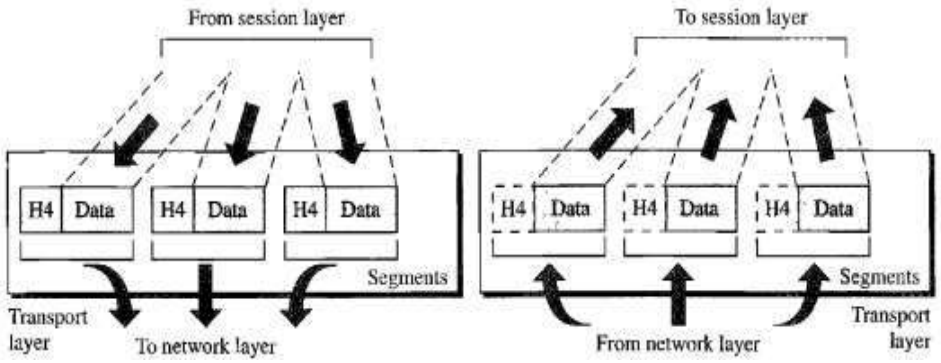
If a packet passes the network boundary that is when the sender and receiver are places in different network then the network layer adds a header that defines the logical address of the devices.

b.Routing

When more than one network connected and to form an internetwork, the connecting devices route the packet to its destination. Network layer provides this mechanism.

4 Transport Layer

The network layer is responsible for the end to end delivery o the entire message. It ensures that the whole message arrives in order and intact. It ensures the error control and flow control at source destination level. The responsibilities are



a. Service point Addressing

A single computer can often run several programs at the same time. The transport layer gets the entire message to the correct process on that computer. It adds a header that defines the port address which used to identify the exact process on the receiver.

b. Segmentation and Reassembly

A message is divided into manageable units called as segments. Each segment is reassembled after received that information at the receiver end. To make this efficient each segment contains a sequence number

c. Connection Control

The transport layer creates a connection between the two end ports. It involves three steps. They are

- Connection establishment
- Data transmission
- Connection discard

d. Flow Control

Flow control is performed at end to end level

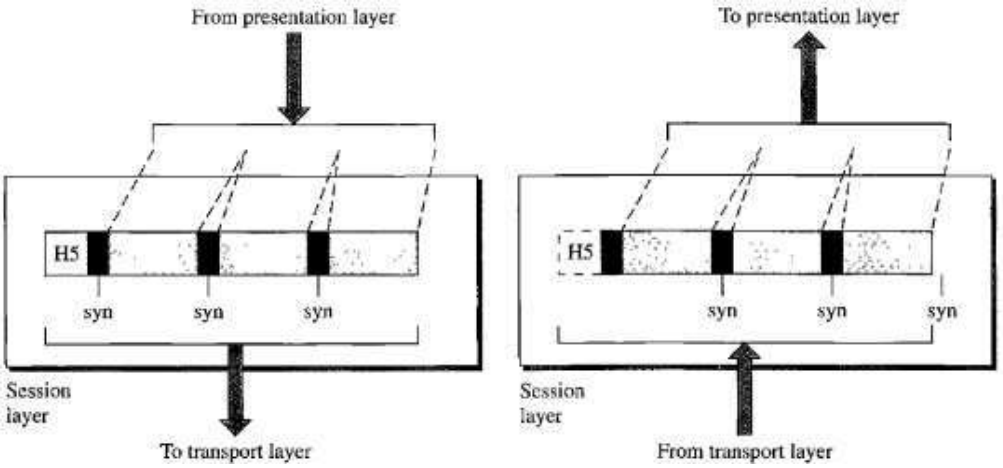
e.Error Control

Error control is performed at end to end level

5 Session Layer

It acts as a dialog controller. It establishes, maintains and synchronizes the interaction between the communication devices.

The responsibilities are,



a. Dialog Control

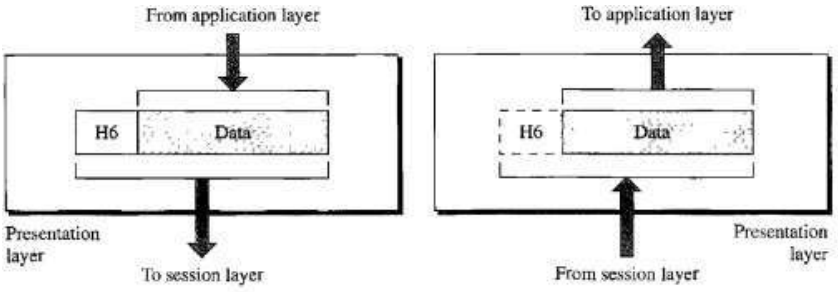
The session layer allows two systems to enter into a dialog. It allows the communication between the devices.

b. Synchronization

It adds a synchronization points into a stream of bits.

6. Presentation Layer

The presentation layer is responsible for the semantics and the syntax of the information exchanged. The responsibilities are,



a. Translation

Different systems use different encoding systems. The presentation layer is responsible for interoperability between different systems. The presentation layer t the sender side translates the information from the sender dependent format to a common format. Likewise, at the receiver side presentation layer translate th information from common format to receiver dependent

format

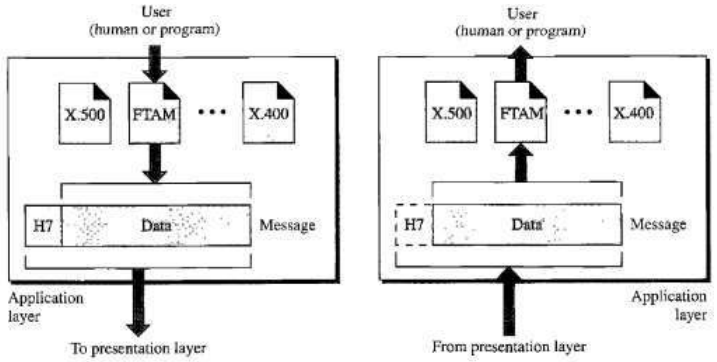
b.Encryption

To ensure security encryption/decryption is used. Encryption means transforms the original information to another form. Decryption means retrieve the original information from the encrypted data. **c.Compression**

It used to reduce the number of bits to be transmitted.

7. Application Layer

The application layer enables the user to access the network. It provides interface between the users to the network. The responsibilities are



a. Network Virtual Terminal

It is a software version of a physical terminal and allows a user to log on to a remote host.

b. File Transfer, Access, and Management

It allows a user to access files in a remote computer, retrieve files, and manage or control files in a remote computer

c. Mail Services

It provides the basis for e-mail forwarding and storage.

d. Directory Services

It provides distributed database sources and access for global information about various objects and services.

1.3.7 TCP/IP REFERENCE MODEL

TCP/ IP stands for Transmission Control Protocol/Internet Protocol. A protocol suite is a large number of related protocols that work together to allow networked computers to communicate layers with same names as OSI Model don't function exactly the same.

1.The Link Layer

The link layer of the TCP/IP reference model corresponds to the first two layers of the ISO/OSI reference model (physical layer and data link layer). Its main task focuses on the secure

transmission of data packets of pooled bit sequences.

2.The Internet Layer

The internet layer, which corresponds to the network layer of the ISO/OSI reference model. Its main responsibility is to enable the data communication of two end systems at a given location in the heterogeneous communication network.

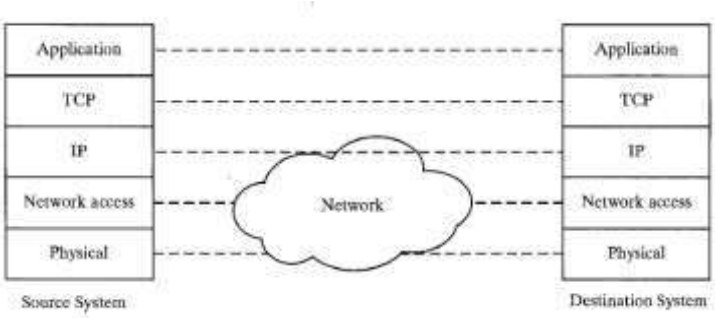
3.The Transport Layer

The transport layer above it corresponds to the layer of the same name in the ISO/OSI reference model. It enables two use programs on different computers in the communication network to exchange reliable and connection-oriented data.

4.The Application Layer

The application layer of the TCP/IP reference model includes the three upper layers of the ISO/OSI reference model and serves as an interface for the actual application programs that wish to communicate with each other over the network

On top of the transport layer is the application layer. It contains all the higher level protocols. The early ones included virtual terminal (TELNET), file transfer (FTP), and electronic mail (SMTP) Many other protocols have been added to these over the years.



Include the Domain Name System (DNS), for mapping host names on their network addresses, HTTP, the protocol for fetching pages on the World Wide Web, and RTP, the protocol for delivering real-time media such as voice or movies.

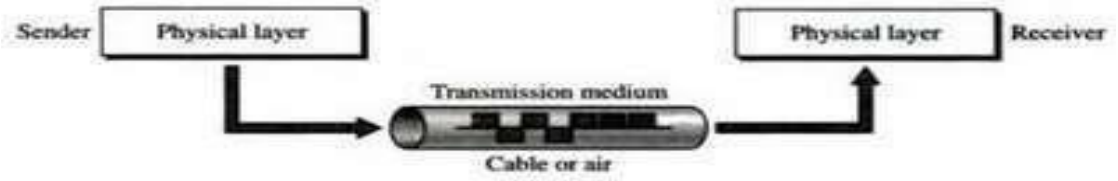
1.4 TRANSMISSION MEDIA

Transmission media are actually located below the physical layer and are directly controlled by the physical layer.

A transmission medium can be broadly defined as anything that can carry information from a source to a destination.

Transmission media can be divided into two broad categories:

1. Guided Medium (Wired)
2. Unguided Medium (Wireless)



1.4.1 Guided Media (Wired Transmission)

Waves are guided along a physical path (e.g., twisted pair, coaxial cable and optical fiber).

1. Twisted Pair

A twisted pair consists of two insulated copper wires arranged in a regular spiral pattern. A wire pair acts as a single communication link

On long-distance links, the twist length typically varies fro 5 to 15 cm. The wires in a pair have thicknesses of from 0.4 to 0.9 mm

Twisted pair comes in two varieties: unshielded and shielded.

Unshielded Twisted Pair (UTP)

Unshielded twisted pair (UTP) is ordinary telephone wire Office buildings, by universal practice, are prewired with exces unshielded twisted pair, more than is needed for simple telephone support. This is the least expensive of all the transmission media commonly used for local area networks and is easy to work with and easy to install

Shielded Twisted Pair

Unshielded twisted pair is subject to external electromagnetic interference, including interference from nearby twisted pair and from noise generated in the environment.

A way to improve the characteristics of this medium is 10 shield the twisted pair with a metallic braid or sheathing that reduces interference.

This shielded twisted pair (STP) provides better performance at higher data rates. However, it is more expensive and more difficult to work with than unshielded twisted pair.

Three categories of UTP cabling:

Category 3: UTP cables and associated connecting hardware whose transmission characteristics are specified up to 16 MHz.

Category 4: UTP cables and associated connecting hardware whose transmission characteristics are specified up to 20 MHz.

Category 5: UTP cables and associated connecting hardware whose transmission characteristics are specified up to 100 MHz.

Applications:

a) Twisted-pair cables are used in telephone lines to provide voice and data channels,

b) Local area networks, such as 10Base-T and 100Base-T, also use twisted-pair cables.

Coaxial Cable:

Another common transmission medium is the **coaxial cable.** Two kinds of coaxial cable are widely used. One kind, 50-ohm cable, is commonly used when it is intended for digital transmission from the start. The other kind, 75-ohm cable, is commonly used for analog transmission and cable television.

A coaxial cable consists of a stiff copper wire as the core, surrounded by an insulating material. The insulator is encased by a cylindrical conductor, often as a closely woven braided mesh. The outer conductor is covered in a protective plastic sheath.

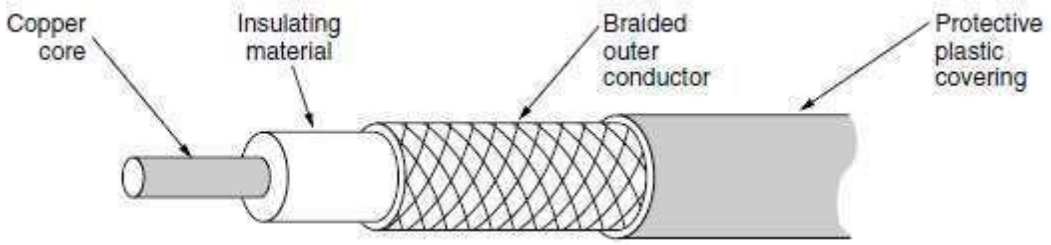


Figure: coaxial cable

The construction and shielding of the coaxial cable give it a good combination of high bandwidth and excellent noise immunity.

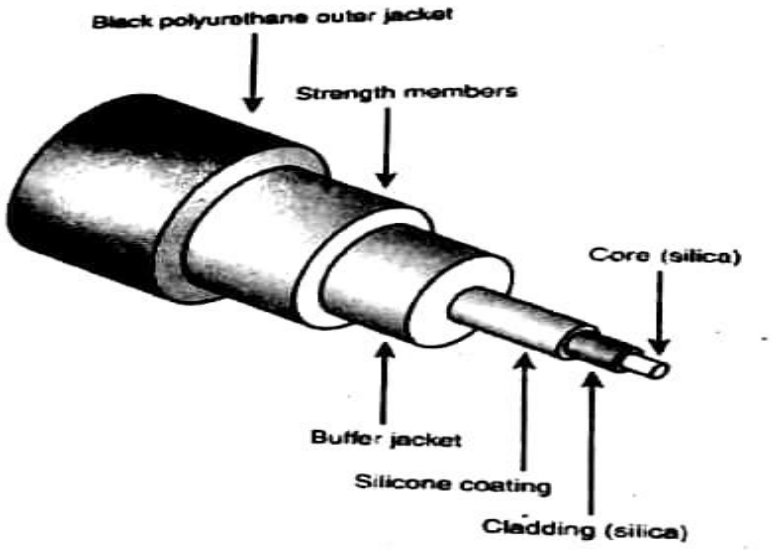
- **Advantages of Coaxial Cable**
  - ✓ Bandwidth is high
  - ✓ Used in long distance telephone lines.
  - ✓ Transmits digital signals at a very high rate of 10Mbps.
  - ✓ Much higher noise immunity
  - ✓ Data transmission without distortion.
  - ✓ The can span to longer distance at higher speeds as they have better shielding when compared to twisted pair cable
- **Disadvantages of Coaxial Cable**
  - ✓ Single cable failure can fail the entire network.
  - ✓ Difficult to install and expensive when compared with twisted pair.
  - ✓ If the shield is imperfect, it can lead to grounded loop.

- **Applications of Coaxial Cable**
  - ✓ Coaxial cable was widely used in analog telephone networks, where a single coaxial network could carry 10,000 voice signals.
  - ✓ Cable TV networks also use coaxial cables. In the traditional cable TV network, the entire network used coaxial cable. Cable TV uses RG-59 coaxial cable.
  - ✓ In traditional Ethernet LANs used it.

3. Optical fiber

An optical fiber is a thin (2 to 125m), flexible medium capable of guiding an optical ray. Various glasses and plastics can he used to make optical fibers,

An optical fiber cable has a cylindrical shape and consists of three concentric sections: the core, the cladding, and the jacket.



Core

The core is the innermost section and consists of one or more very thin strands, or fibers, made of glass or plastic, the core has diameter in the range of 8 to 100um.

Cladding

Each fiber is surrounded by its own cladding, a glass or plastic coating that has optical properties different from those of the interface between the core and cladding light that would otherwise escape the core. core The acts as a reflector to confine

Jacket

The jacket is composed of plastic and other material layered to protect against moisture, abrasion, crushing, and other environmental dangers.

Applications:

- One of the most significant technological breakthroughs in data transmission has been the development of practical fiber optic communications systems,
- Use in military applications is growing.
- The continuing improvements in performance and decline in prices.
- Use in medical field.

Comparison of Fiber optic and Copper cable

Properties	Fiber	Copper
Bandwidth	Higher	Lower
Distance between repeaters	30 KM	5 Km
Interference	Low	High
Physical	Smaller/Lighter	-
Flow	Uni-directional	Bi-directional

Short Questions and Answers

1. Define Computer Network.

A network is a set of devices connected by physical media links. A network is recursively is a connection of two or more nodes (normally computers) by a physical link or two or more networks connected by one or more nodes.

2. What is a Link?

At the lowest level, a network can consist of two or more computers directly connected by some physical medium such as coaxial cable or optical fiber. Such a physical medium is called as Link.

3. What is a node?

A network can consist of two or more network devices (such as computer, laptop, routers, switches, bridges, servers and printers) directly connected by some physical medium. The connected devices are called as Nodes.

4. What is meant by data communication?

Data communication is process of exchanging data between two devices through a communication medium in a meaningful way.

5. What are the fundamental characteristics to be followed in effective communication?

To provide the effective communication system, the following four fundamental characteristics must be followed;

a. Delivery
b. Accuracy
c. Timeliness
d. Jitter
e. Define Jitter.

In network the data are split into smaller groups (packets) and send them separately.
The variation of the arrival between two packets is referred as jitter.

6. List out the essential components of the communication system.

a. Data/Message
b. Source
c. Destination
d. Medium
e. Protocol
f. Define Data Flow.

The data flow defines the flow direction of the data between source and destination.
The data flow may be either simplex or half-duplex or full duplex.

7. What is meant by Half-Duplex data transmission?

In half-duplex mode, the data can be transmitted on both directions (device 1 to device 2 or device 2 to device 1) but not at the same time. One device can send and another one can receive at a time. The example is walkie-talkie. The entire medium is used for the one-way transmission.

8. What is meant by Full-Duplex data transmission?

In full-duplex mode, the data can be transmitted on both directions (device 1 to device 2 and device 2 to device 1) at the same time (One device can send and another one can receive at a time. The example is telephone communication. In this, the entire medium is divided for the two-way transmission.

9. List out few applications of computer networks

a) Business Applications
b) Home Applications

c) Mobile Users

d) Social issues

10. What is point-point link?

If the physical links are directly connected to a pair of nodes it is said to be point-point link.

11. What is Multiple Access?

If the physical links are shared by more than two nodes, it is said to be Multiple Access.

12. Mention the types of transmission technology.

There are two types of transmission technology that are in widespread use: Broadcast links and point-to-point links.

13. Define packets?

To go from the source to the destination on a network made up of point-to-point links, short messages, called packets.

14. What is unicasting?

Transmission with exactly one sender and exactly one receiver is sometimes called unicasting.

15. What is Broadcasting?

Broadcast systems usually also allow the possibility of addressing a packet to all destinations by using a special code in the address field. When a packet with this code is transmitted, it is received and processed by every machine on the network. This mode of operation is called broadcasting.

16. What is Multicasting?

Some broadcast systems also support transmission to a subset of the machines, which known as multicasting.

17. What is meant by service in layered model?

Service is a set of primitives (operations) that a layer provides to the layer above it. The service defines what operations the layer is prepared to perform on behalf of its users, but it says nothing at all about how these operations are implemented. A service relates to an interface between two layers, with the lower layer being the service provider and the upper layer being the service user.

18. Define Protocol.

Protocol is a set of rules governing the format and meaning of the packets, or messages that are exchanged by the peer entities within a layer. Entities use protocols to implement their service definitions.

19. What are the key elements of protocol?

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

20. What is meant by syntax?

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

21. What is meant by semantics?

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

22. What is meant by timing?

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

23. What are the responsibilities of data link layer?

Specific responsibilities of data link layer include the following.

a) Framing

b) Physical addressing

c) Flow control

d) Error control

e) Access control

24. Why are protocols needed?

In networks, communication occurs between the entities in different systems. Two entities cannot just send bit streams to each other and expect to be understood. For communication, the entities must agree on a protocol. A protocol is a set of rules that govern data communication.

25. Group the OSI layers by function.

The seven layers of the OSI model belonging to three subgroups. Physical, datalink and network layers are the network support layers; they deal with the physical aspects of moving data from one device to another. Session, presentation and application layers are the user support layers; they allow interoperability among unrelated software systems. The transport layer ensures end-to-end reliable data transmission.

26. What are header and trailers and how do they get added and removed?

Each layer in the sending machine adds its own information to the message it

receives from the layer just above it and passes the whole package to the layer just below it. This information is added in the form of headers or trailers. Headers are added to the message at the layers 6,5,4,3, and 2. A trailer is added at layer2. At the receiving machine, the headers or trailers attached to the data unit at the corresponding sending layers are removed, and actions appropriate to that layer retaken.

27. The transport layer creates a communication between the source and destination.

What are the three events involved in a connection?

Creating a connection involves three steps: connection establishment, data transfer and connection release.

28. What is a switch?

A switch is a networking device that manages networked connections between devices on a star network.

29. Define Bluetooth.

Bluetooth is a wireless technology standard for exchanging data over short distances (using short-wavelength UHF radio waves in the ISM band from 2.4 to 2.485 GHz) from fixed and mobile devices and building personal area networks (PANs).

30. What is LAN?

A LAN is a privately owned network that operates within and nearby a single building like a home, office or factory. LANs are widely used to connect personal computers and consumer electronics to let them share resources (e.g., printers) and exchange information.

31. List out Advantages of Ethernet.

a. Inexpensive

b. Easy to install

c. Supports various writing technologies.

32. What are the limitations of bridges?

a. Scale

b. Heterogeneity

33. Define router.

Router is a network layer device that connects networks with different physical media and translates between different network architecture.

34. Define Transmission Lines.

Its move bits between machines. They can be made of copper wire, optical fiber, or even radio links. Most companies do not have transmission lines lying about, so instead they lease the lines from a telecommunications company.

35. Define gateway.

The general name for a machine that makes a connection between two or more networks and provides the necessary translation, both in terms of hardware and software, is a gateway. Gateways are distinguished by the layer at which they operate in the protocol hierarchy.

36. Define Signals

Signal is a physical representation of data by means of analog or digital. To be transmitted, data must be transformed to electromagnetic signals.

37. What is meant by periodic and nonperiodic signals?

Both analog and digital signals can take one of two forms: periodic or nonperiodic (sometimes refer to as aperiodic, because the prefix a in Greek means "non").

A periodic signal completes a pattern within a measurable time frame, called a period, and repeats that pattern over subsequent identical periods. The completion of one full pattern is called a cycle. A nonperiodic signal changes without exhibiting a pattern or cycle that repeats over time.

38. What is meant by bit rate?

The bit rate is the number of bits sent in 1s, expressed in bits per second (bps). The bit rate (instead of frequency)-is used to describe digital signals

39. Define throughput or data transfer rate.

In computer network, throughput is defined as the actual number of bits that flows through a network connection in a given period of time. Throughput is always less than or equal to bandwidth but can never exceed bandwidth.

40.What are the factors that the throughput of a computer network?

In a computer network, the throughput can be affected by many factors as listed below:

- Network congestion due to heavy network usage.
- Too many users are accessing the same server.
- Low bandwidth allocation between network devices.
- Medium loss of a computer network.
- Resources (CPU, RAM) of network devices.

40. List the Guided Media used in computer network.

There are five types in guided media used in computer network.

a. Magnetic Media
b. Twisted Pairs
c. Coaxial Cable
d. Power Lines
e. Fiber Optics

Explanatory Questions

1. What are the 4 types of network? (5)
2. Discuss about protocol hierarchies (5).
3. Explain the service primitives used in connection oriented service (5).
4. Differentiate the OSI and TCP Reference models (5).
5. How to classify the Computer Network. Explain with its merits and demerits. (10)
6. Briefly Discuss about the ISO reference model (10)
7. Explain about the TCP/IP Reference model (10)
8. Discuss about the signals (5).
9. Explain the guided transmission media with necessary diagrams (10).
10. Discuss about the cable television (10).

Objective Questions

1. The frequency is measured by unit

   (a) Hertz
   (b) bit
   (c) byte
   (d) meter

   Answer : a

2. Bandwidth of channel is calculated by

   (a) Difference between lower bound frequency and upper bound frequency
   (b) upper bound frequency
   (c) lower bound frequency
   (d) Difference between lower amplitude and upper amplitude

   Answer : a

3. Hertz is defined as

   (a) One cycle per bit
   (b) One cycle per second
   (c) One cycle per byte
   (d) All the above

Answer : b

4. What happens to the bandwidth frequency range when the quality factor increases?

   (a) Becomes zero

   (b) Increases

   (c) Decreases

   (d) Remains the same

   Answer : b

5. The bandwidth of wireless radio LAN is

   (a) 24Mbps

   (b) 2 Mbps

   (c) 4 Mbps

   (d) 8 Mbps

   Answer : b

6. The frequency range of wireless LAN is

   (a) 900 MHz bands

   (b) 2GHz bands

   (c) 5 GHz bands

   (d) All of these

7. Signals are transmitted in terms

   (a) Raw bits

   (b) Electromagnetic waves

   (c) Electronics waves

   (d) Electrical waves

8. What is the bandwidth of the FM radio channel?

   (a) 200 MHz

   (b) 200 kHz

   (c) 200 Hz

   (d) 200 GHz

9. The audible bandwidth of human ear ranges is _____

   (a) 20 Hz to 20,000Hz

   (b) 20 kHz to 20,000kHz

   (c) 20 MHz to 20,000MHz

   (d) None of the above

10. What is the frequency range used in RADAR?

(a) 1 MHz

(b) 3 MHz

(c) 3 to 4 MHz

(d) 1 to 3 MHz

11. A given signal has frequencies of 3125 MHz, 635 MHz, 2000MHz and 7000MHz. Determine the bandwidth of the signal?

(a) 5365 MHz

(b) 5000 MHz

(c) 6365 MHz

(d) 3875 MHz

12. The frequency of human heart rate is

(a) 1 Hz

(b) 2Hz

(c) 1.2 Hz

(d) 1.3 Hz

13. The hertz is named from

(e) Heinrich Hertz

(a) Hillarous Hertz

(b) Hamilton Hertz

(c) Henrock Hertz

14. The modulation efficiency in bit/s defined as

(a) The gross bitrate (including any error-correcting code) divided by the bandwidth.

(b) The gross bitrate (excluding any error-correcting code) divided by the bandwidth.

(c) The gross bitrate (including any error-correcting code) divided by the throughput.

(d) The gross bitrate (excluding any error-correcting code) divided by the bandwidth

15. The throughput of communication line is defined as

(a) Maximum amount of data transferred in period of time

(b) Actual data transferred in period of time

(c) Minimum amount of data transferred in period of time

(d) All the above

16. The bit rate of signal is 3000bps. If each signal unit carries 6 bits, the baud rate of the signal rates is_.

(a) 500 baud/s

(b) 1000 baud/sec

(c) 3000 baud/sec

(d) 18000 baud/sec

Answer : a

17. The period of signal is 10 ms. What is the frequency in hertz?

(a) 10

(b) 100

(c) 1000

(d) 10000

Answer : b

18. An analog signal carries 4 bits in each signal unit. If 1000 signal units are sent per second, then baud rate and bit rate of the signal are and _____

(a) 4000 bauds / sec & 1000 bps

(b) 2000 bauds / sec & 1000 bps

(c) 1000 bauds / sec & 500 bps

(d) 1000 bauds / sec & 4000 bps

Answer : d

19. What is the period for a frequency of 60 Hz?

(a) 1s

(b) 1ms

(c) 16.67ms

(d) 10 ms

Answer : c

20. An analog signal has a bit rate of 6000 bps and a baud rate of 2000 baud. How many data elements are carried by each signal element?

(a) 0.336 bits/baud

(b) 3 bits/baud

(c) 120,00,000 bits/baud

(d) None of the above

Answer : b

21. Which signal has a wider bandwidth, a sine wave with a frequency of 100 Hz or a sine wave with a frequency of 200 Hz?

(a) 100Hz

(b) 200Hz

(c) same

(d) different

Answer : c

22. A device is sending out data at the rate of 1000 bps. How long does it take to send a file of 100,000 characters?

(a) 800s

(b) 80s

(c) 8 s

(d) 8 minutes

Answer : a

23. A TV channel has a bandwidth of 6 MHz. If we send a digital signal using one channel, what are the data rates if we use one five harmonics?

(a) 2 Mbps

(b) 2.4 Mbps

(c) 6Mbps

(d) 30 Mbps

Answer : b

24. If the bandwidth of the channel is 5 Kbps, how long does it take to send a frame of 100,000 bits out of this device?

(a) 10s

(b) 200s

(c) 20s

(d) 2s

Answer :c

25. A network with bandwidth of 8 Mbps can pass only an average of 20,000

frames per minute with each frame carrying an average of 12,000 bits. What is the throughput of this network?

(a) 8 Mbps
(b) 4 Mbps
(c) 12 Mbps
(d) 20 Mbps

Answer : b

26. A file contains 2 million bytes. How long does it take to download this file using a 56- Kbps channel? 1-Mbps channel?

(a) 285.7s, 2s
(b) 285.7s, 16s
(c) 571s, 32s
(d) 571s,16s

Answer : b

27. What is the bit rate for transmitting uncompressed 800 x 600 pixel colour frames with 8 bits/pixel at 40 frames/second?

(a) 2.4 Mbps
(b) 15.36 Mbps
(c) 153.6 Mbps
(d) 1536 Mbps

Answer : c

28. What is the transmission time of a packet sent by a station if the length of the packet is 1 million bytes and the bandwidth of the channel is 200 Kbps?/

(a) 4s
(b) 40s
(c) 4 mins
(d) 5s

Answer : b

29. A periodic signal completes one cycle in 0.001s. What is the frequency?

(a) 1Hz
(b) 100 Hz
(c) 1 kHz

(d) 1 MHz

Answer : c

30. If the bandwidth of the signal is 5KHz and the lowest frequency is 52KHz, what is the highest frequency?

(a) 5 KHz
(b) 52 KHz
(c) 47 KHz
(d) 57 KHz

Answer : d

31. The period of cycle is 220ns. What is the corresponding frequency in MHz?

(a) 50 MHz
(b) 5 MHz
(c) 50 KHz
(d) 500 MHz

Answer : b

32. How many KHz are in one GHz?

(a) 10^6 *KHz*
(b) 10^3 KHz
(c) 1000 KHz
(d) 10000KHz

Answer : a

33. The number of layers in Internet protocol stack

a) 5
b) 7
c) 6
d) None of the mentioned

Answer: a

Explanation: There are five layers in the Internet Protocol stack. The five layers in Internet Protocol stack is Application, Transport, Network, Data link and Physical layer.

34. The number of layers in ISO OSI reference model

a) 5

b) 7

c) 6

d) None of the mentioned

Answer: b

Explanation: The seven layers in ISO OSI reference model is Application, Presentation, Session, Transport, Network, Data link and Physical layer.

35. This layer is an addition to OSI model when compared with TCP IP model

a) Application layer

b) Presentation layer

c) Session layer

d) Both Session and Presentation layer

Answer: d

Explanation: The only difference between OSI model and TCP/IP model is that in OSI model two layers namely Presentation and Session layer have been added.

36. Application layer is implemented in

a) End system

b) NIC

c) Ethernet

d) None of the mentioned

Answer: a

Explanation: Not only application layer, but presentation layer, session layer and transport layer are also implemented in the end system.

37. Transport layer is implemented in

a) End system

b) NIC

c) Ethernet

d) None of the mentioned

Answer: a

Explanation: Application, Presentation, Session and Transport layer are implemented in the end system.

38. The functionalities of presentation layer includes

    a) Data compression

    b) Data encryption

    c) Data description

    d) All of the mentioned

Answer: d

Explanation: Some functions of the presentation layer include character-code translation, data conversion, data encryption and decryption, and data translation.

39. Delimiting and synchronization of data exchange is provided by

    a) Application layer

    b) Session layer

    c) Transport layer

    d) Link layer

Answer: b

Explanation: The session layer provides the mechanism for opening, closing and managing a session between end-user application processes. The session layer 5 is responsible for establishing managing synchronizing and terminating sessions.

40. In OSI model, when data is sent from device A to device B, the 5th layer to receive data at B is

    a) Application layer

    b) Transport layer

    c) Link layer

    d) Session layer

Answer: d

Explanation: In OSI reference model, the fifth layer is Session layer. Session layer provides the mechanism for opening, closing and managing a session between end-user application processes.

41. In TCP IP Model, when data is sent from device A to device B, the 5th layer to receive data at B is

a) Application layer

b) Transport layer

c) Link layer

d) Session layer

Answer: a

Explanation: In TCP/IP model, the fifth layer is application layer. when data is sent from device A to device B, the 5th layer to receive data at B is application layer.

42. In the OSI model, as a data packet moves from the lower to the upper layers, headers are

_____

a) Added

b) Removed

c) Rearranged

d) None of the mentioned

Answer: b

Explanation: In OSI reference model, when data packet moves from lower layers to higher layer, headers get removed. Whereas when data packet move from higher layer to lower layers, headers are added.

43. OSI stands for

a) open system interconnection

b) operating system interface

c) optical service implementation

d) none of the mentioned

Answer: a

Explanation**:** OSI is the abbreviation for Open System Interconnection. OSI model provides a structured plan on how applications communicate over a network, which also helps us to have a structured plan for troubleshooting.

44. The OSI model has_____layers.

a) 4

b) 5

c) 6

d) 7

Answer: d

Explanation: In OSI reference model, there are 7 layers namely Application, Presentation, Session, Transport, Network, Data Link and Physical layer.

45. TCP/IP model does not have_____layer but OSI model have this layer

a) session layer

b) transport layer

c) application layer

d) None of the mentioned

Answer: a

Explanation: In OSI reference model, there are two layers which are not present in TCP/IP model. They are Presentation and Session layer.

46. Which layer links the network support layers and user support layers

a) session layer

b) data link layer

c) transport layer

d) network layer

Answer: c

Explanation: Physical, data link and network layers are network support layers and session, presentation and application layers are user support layers.

47. Which address is used in an internet employing the TCP/IP protocols?

a) physical address and logical address

b) port address

c) specific address

d) all of the mentioned

Answer: d

Explanation: All of the mentioned above addresses are used in TCP/IP protocol. All the addressing scheme, that is physical (MAC) and logical address, port address and specific address are employed in both TCP/IP model and OSI model.

48. TCP/IP model was developed the OSI model.

a) prior to

b) after

c) simultaneous to

d) none of the mentioned

Answer: a

Explanation: Several TCP/IP prototypes were developed at multiple research centers between 1978 and 1983, whereas OSI reference model was developed in the year 1984.

49. Which layer is responsible for process to process delivery?

a) network layer

b) transport layer

c) session layer

d) data link layer

Answer: b

Explanation: The role of Transport layer (Layer 4) is to establish a logical end to end connection between two system in a network. The protocols used in Transport layer is TCP and UDP.

50. Which address identifies a process on a host?

a) physical address

b) logical address

c) port address

d) specific address

Answer: c

Explanation: A port number is a way to identify a specific process to which an Internet or other network message is to be forwarded when it arrives at a server.

51. Which layer provides the services to user?

a) application layer

b) session layer

c) presentation layer

d) none of the mentioned

Answer: a

Explanation: In networking, a user mainly interacts with application layer to create and send information to other computer or network.

52. Transmission data rate is decided by

a) network layer

b) physical layer

c) data link layer

d) transport layer

Answer: b

Explanation: Physical layer is a layer 1 device which deals with network cables or the standards in use like connectors, pins, electric current used etc. Basically the transmission speed is determined by the cables and connectors used. Hence it is physical layer that determines the transmission speed in network.

2. Data Link Layer

2.1Data Link Layer

The data link layer is the protocol layer in a program that handles the moving of data into and out of a physical link in a network. The data link layer is Layer 2 in the Open Systems Interconnection (OSI) architecture model for a set of telecommunication protocols. Data bits are encoded, decoded and organized in the data link layer, before they are transported as frames between two adjacent nodes on the same LAN or WAN.

The data link layer also determines how devices recover from collisions that may occur when nodes attempt to send frames at the same time. The *Figure 2.1* shows the relationship of the Data Link Layer to the network layer and physical layer.

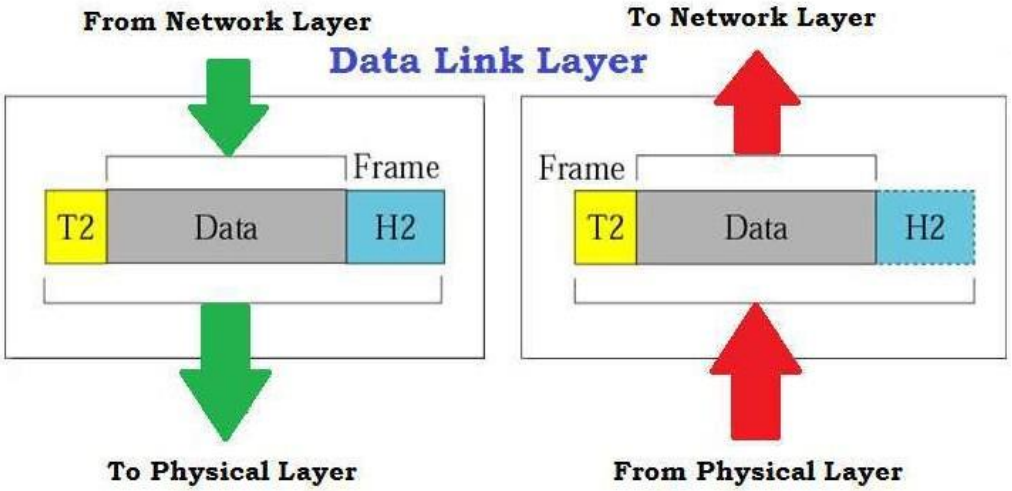


Figure: Relationship between data link layer with physical layer and network layer

2.1.1Data Link Layer Design Issues

The data link layer uses the services of the physical layer to send and receive bits over communication channels. It has a number of functions, including:

- Providing a well-defined service interface to the network layer.
- Dealing with transmission errors.
- Regulating the flow of data so that slow receivers are not swamped by fast senders.

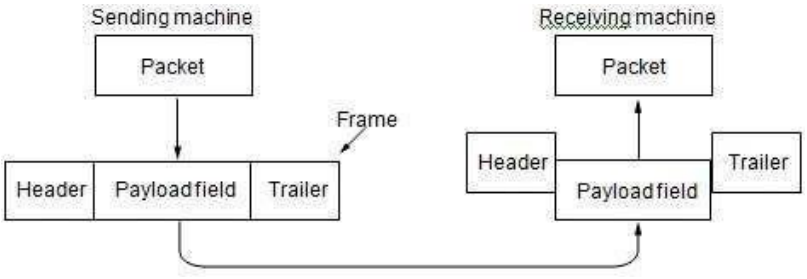


Figure : Relationship between packets and frame

To accomplish these goals, the data link layer takes the packets it gets from the network layer and encapsulates them into frames for transmission. Each frame contains a frame header, a payload field for holding the packet, and a frame trailer as shown in figure Frame management forms the heart of what the data link layer does.

2.1.2Services Provided to the Network Layer

The function of the data link layer is to provide services to the network layer. The principal service is transferring data from the network layer on the source machine to the network layer on the destination machine. On the source machine is on entity, call it a process, in the network layer that hands some bits to the data link layer for transmission to the destination. 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 there, as shown in *Figure*(*a).* The actual transmission follows the path of *Figure 2.3*, but it is easier to think in terms of two data link layer processes communicating using a data link protocol. For this reason, we will implicitly use the model of *Figure (b).*

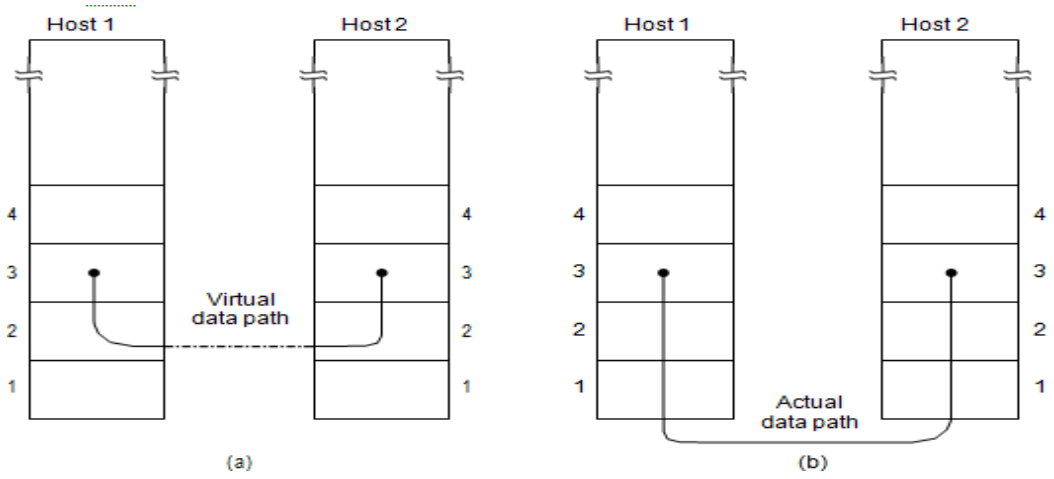


Figure (a) Virtual communication. (b) Actual communication.

The data link layer can be designed to offer various services. The actual ser- vices that are offered vary from protocol to protocol. Three reasonable possibilities that we will consider in turn are:

1. Unacknowledged connectionless service.
2. Acknowledged connectionless service.
3. Acknowledged connection-oriented service

1.Unacnowledged connectionless service.

Unacknowledged connectionless service consists of having the source machine send independent frames to the destination machine without having the destination machine

acknowledge them.

No logical connection is established beforehand or released afterward. If a frame is lost due to noise on the line, no attempt is made to detect the loss or recover from it in the data link layer. This class of service is appropriate when the error rate is very low so that recovery is left to higher layers. It is also appropriate for real-time traffic, such as voice, in which late data are r. worse than bad data. Most LANs use unacknowledged connectionless service in the data link layer.

2.Acknowledged connectionless service.

When this service is offered, there are still no logical connections used, but each frame sent is individually acknowledged. In this way, the sender knows whether a frame has arrived correctly. If it has not arrived within a specified time interval, it can be sent again. This service is useful over unreliable channels, such as wireless systems.

3.Connection-Oriented service.

The most sophisticated service the data link layer can provide to the network layer is connection-oriented service. With this service, the source and destination machines establish a connection before any data are transferred. Each frame sent over the connection is numbered, and the data link layer guarantees that each frame sent is indeed received. Furthermore, it guarantees that each frame is received exactly once and that all frames are received in the right order.

When connection-oriented service is used, transfers go through three distinct phases.

Phase 1: Connection is established

Phase 2: One or more frames are actually transmitted.

Phase 3 : The connection is released, freeing up the variables, buffers and other resources used to maintain the connection.

Framing

To provide service to the network layer, the data link layer must use the service provided to it by the physical layer. What the physical layer does is accept a raw bit stream and attempt to deliver it to the destination. If the channel is noisy, as it is for most wireless and some wired links, the physical layer will add some redundancy to its signals to reduce the bit error rate to a tolerable level. However, the bit stream received by the data link layer is not guaranteed to be error free.

The usual approach is for the data link layer to break up the bit stream into discrete frames, compute a short token called a checksum for each frame, and include the checksum in the frame when it is transmitted. When a frame arrives at the destination, the checksum is recomputed.

Breaking up the bit stream into frames is more difficult than it at first appears. A good design must make it easy for a receiver to find the start of new frames while using little of the channel bandwidth. We will look at four methods:

1. Byte count.
2. Flag bytes with byte stuffing.
3. Flag bits with bit stuffing.
4. Physical layer coding violations.

1.Byte count

The byte count method uses a field in the header to specify the number of bytes in the frame. When the data link layer at the destination sees the byte count, it knows how many bytes follow and hence where the end of the frame is. This technique is shown in *Figure* (a) for four small example frames of sizes 5, 5, 8, and 8 bytes, respectively.

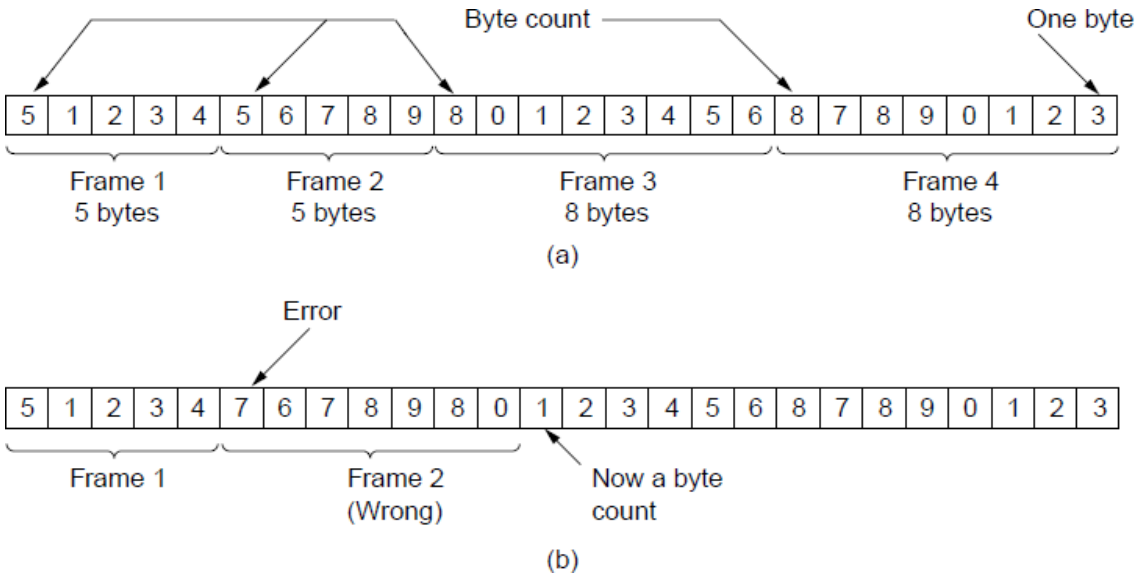


Figure : A byte stream. (a) Without errors. (b) With one error.

Frame Error

The trouble with this algorithm is that the count can be garbled by a transmission error. For example, if the byte count of 5 in the second frame of *Figure* (b) becomes a 7 due to a single bit flip, the destination will get out of synchronization. It will then be unable to locate the correct start of the next frame. Even if the checksum is incorrect so the destination knows that the frame is bad, it still has no way of telling where the next frame starts.

Sending a frame back to the source asking for a retransmission does not help either, since the destination does not know how many bytes to skip over to get to the start of the retransmission. For this reason, the byte count method is rarely used by itself.

2.Flag bytes with byte stuffing.

The second framing method gets around the problem of resynchronization after an error by having each frame start and end with special bytes. Often the same byte, called a flag byte, is used as both the starting and ending delimiter. This byte is shown in Fig. (a) as FLAG. Two consecutive flag bytes indicate the end of one frame and the start of the next. Thus, if the receiver ever loses synchronization it can just search for two flag bytes to find the end of the current frame and the start of the next frame.

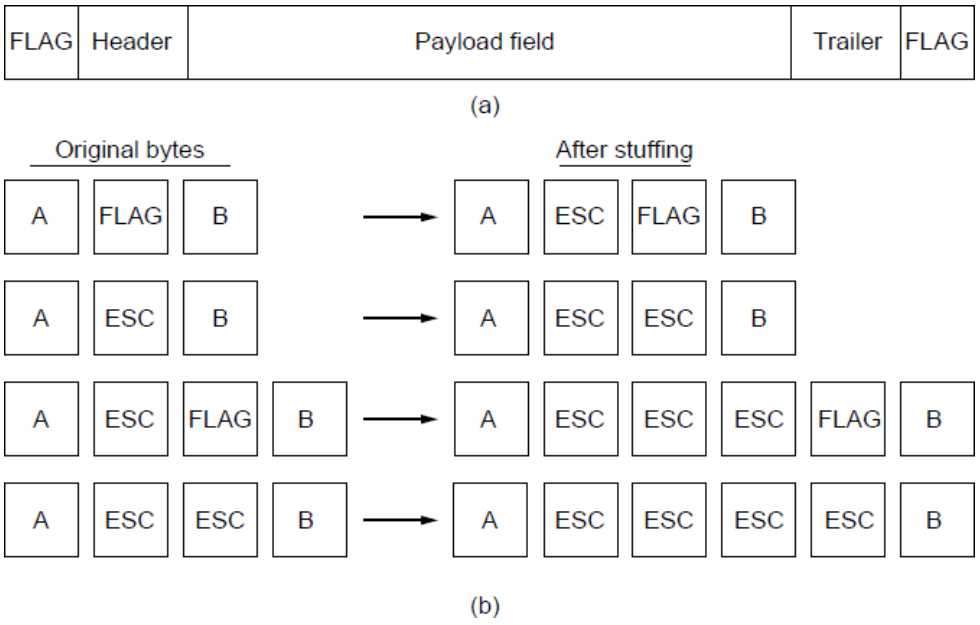


Figure (a) A frame delimited by flag bytes. (b) Four examples of byte sequences before and after byte stuffing.

Problem in Flag

- ✓ Flag methods used for synchronization.
- ✓ The 'flag' bit pattern may occur in data transformation.
- ✓ To avoid this, byte stuffing is used with 'ESC' byte stuffing.
- ✓ Used in PPP protocol.
- ✓ Not suitable for 16-bit characters (UNICODE).

3.Flag bits with bit stuffing.

The third method of delimiting the bit stream gets around a disadvantage of byte stuffing, which is that it is tied to the use of 8-bit bytes. Framing can be also be done at the bit level, so frames can contain an arbitrary number of bits made up of units of any size. It was developed for the once very popular HDLC (High- level Data Link Control) protocol.

Each frame begins and ends with a special bit pattern, 01111110 or 0x7E in hexadecimal. This pattern is a flag byte. When-ever the sender's data link layer encounters five consecutive 1s

in the data, it automatically stuffs a 0 bit into the outgoing bit stream.

When the receiver sees five consecutive incoming 1 bits, followed by a 0 bit, it automatically destuffs (i.e., deletes) the 0 bit. Just as byte stuffing is completely transparent to the network layer in both computers, so is bit stuffing. If the user data contain the flag pattern, 01111110, this flag is transmitted as 011111010 but stored in the receiver's memory as 01111110.

With bit stuffing, the boundary between two frames can be unambiguously recognized by the flag pattern. Thus, if the receiver loses track of where it is, all it has to do is scan the input for flag sequences, since they can only occur at frame boundaries and never within the data.

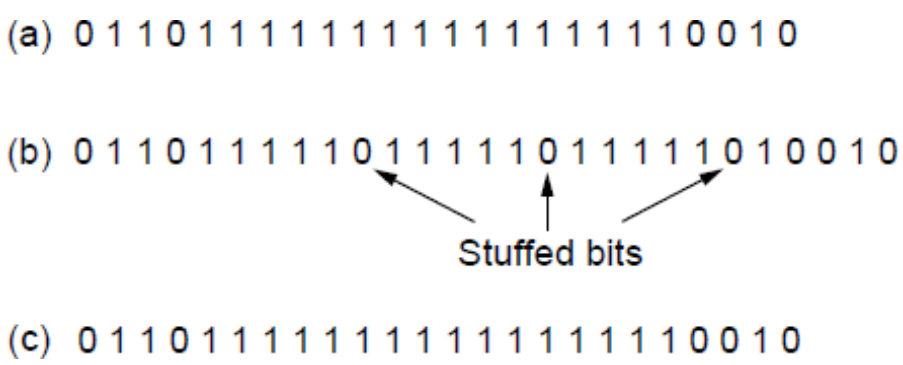


Figure. Bit stuffing. (a) The original data. (b) The data as they appear on the line. (c) The data as they are stored in the receiver's memory after destuffing.

4.Physical layer coding violations

Many data link protocols use a combination of these methods for safety. A common pattern used for Ethernet and 802.11 is to have a frame begin with a well-defined pattern called a preamble. This pattern might be quite long (72 bits is typical for 802.11) to allow the receiver to prepare for an incoming packet. The preamble is then followed by a length (i.e., count) field in the header that is used to locate the end of the frame.

Error Control

The next issue in the data link layer is error control. The error may be happened during the transmission. The errored frames are dropped by the receiver and acknowledgement are not sent. The Acknowledgment (ACK) used for reliable delivery. If frame or ACK is lost, no ACK is sent to sender. In this case Sender uses timer to react with average round trip time (RTT) to retransmit the frame. If ACK is lost, receiver receives multiple copies of same frame. To identify multiple copies and remove the duplicated copies of the frame, sequence number is used in the frames.

Flow Control

Flow control is a technique that allows two stations working at different speeds to communicate with each other. It is a set of measures taken to regulate the amount of data that a sender sends so that a fast sender does not overwhelm a slow receiver.

In data link layer, flow control restricts the number of frames the sender can send before it waits for an acknowledgment from the receiver. Two approaches are commonly used.

- **Feedback based Flow Control** - the sender sends frames after it has received acknowledgments from the user. This is used in the data link layer.
- **Rate based Flow Control** - These protocols have built in mechanisms to restrict the rate of transmission of data without requiring acknowledgment from the receiver. Used in the network layer and the transport layer.

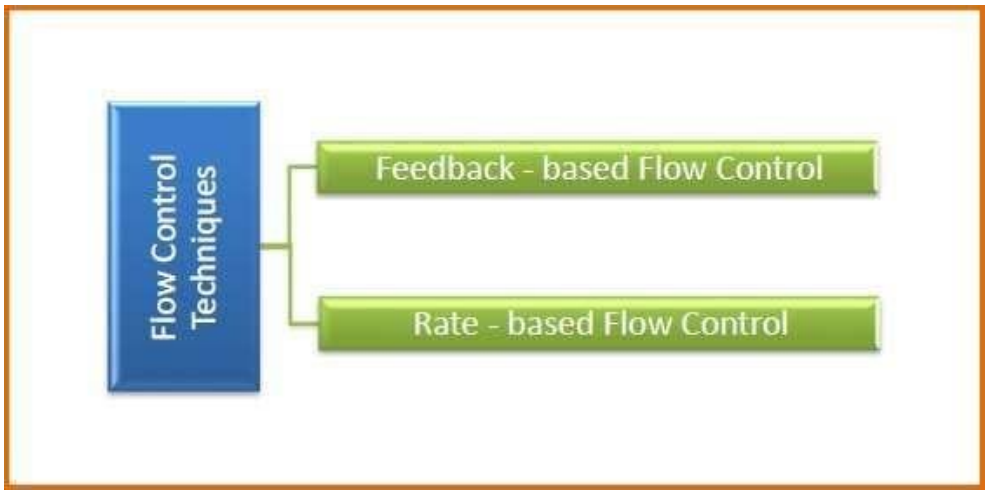


Figure : Approaches of Flow Control

2.2Channel Allocation Problem

The network connections are categorized into two: point-to-point connections and broadcast connections. In point-to-point connections, the communication is carried out between exactly two persons. Hence, the channel is allocated only for these two persons. But, in a broadcast network, the main problem is to determine the allocation of channel when many users trying to access. These broadcast channels are sometime called as multiple access channel or random-access channel.

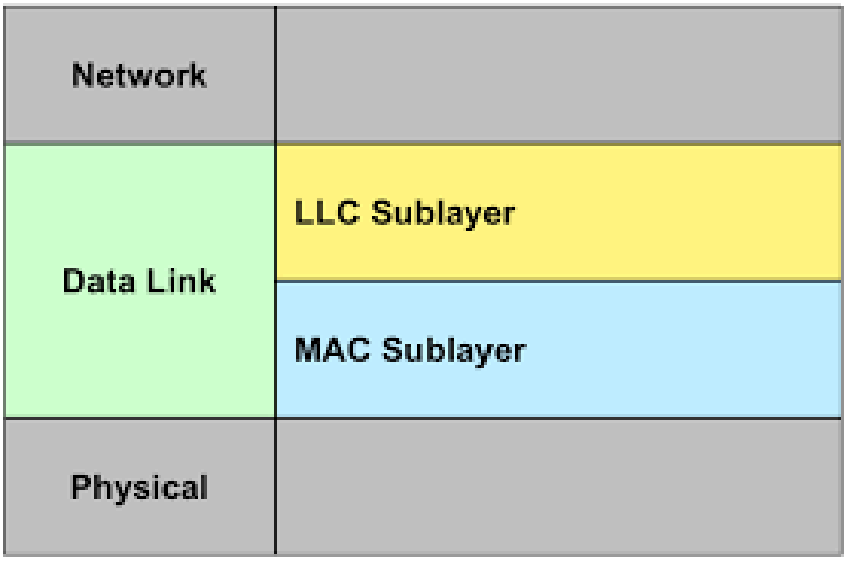


Figure :Sub Layers of Data Link Layer

The protocols used to determine who goes next on a multiaccess channel belong to a sublayer of the data link layer called the MAC (Medium Access Control) sublayer. The MAC sublayer is especially important in LANs, many of which use a multiaccess channel as the basis for communication. WANs, in contrast, use point-to-point links, except for satellite networks. The Figure 2.8 shows the sub layers of data link layer. Technically, the MAC sublayer is the bottom part of the data link layer.

The main aim of the channel allocation is how to allocate a single broadcast channel among competing users. The allocation is divided into static and dynamic channel allocation. We look into these in detail.

2.2.1Static Channel allocation

In this scheme a Frequency Division Multiplexing (FDM) is used for allocating a single channel among competing users. For example, if we have N users, the bandwidth will be divided into N equal-size portions, then each user being assigned one portion. Since each user has a private frequency band, there is no interference between users.

It is not efficient to divide into fixed number of chunks. Now let us divide the single channel into N independent subchannels, each with capacity C/N bps. The mean input rate on each of the subchannels will now be λ/N.

- Advantage : FDM is a simple and efficient allocation mechanism.
- Disadvantage : Waste of resources when the traffic is bursty, or the channel is lightly loaded

2.2.2Dynamic Channel allocation

In dynamic channel allocation schemes, frequency channels are not permanently allotted to any user. Channels are assigned to the user as needed depending upon the network environment. The five key assumptions in dynamic channel allocation are:

1. ***Station Model*** : The model consists of *N* independent stations (terminals such as computers, telephones or persona communicators) each with a program or user that generates frames for transmission. Once a frame has been generated, the station is blocked and does nothing until the frame has been successfully transmitted.
2. ***Single Channel Assumption***: A single channel is available for communication. All stations can send or receive on the channel. All stations are equivalent, although protocol software may assign priorities to them.
3. ***Collision Assumption***: If two frames are transmitted simultaneously, they overlap. This event is called a collision. All stations can detect collisions.
    - A collided frame must be retransmitted. There are no errors other than those generated by collisions.

4. Transmission time division

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

b. *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.

5. Carrier Sense

a. *With carrier sense* : Stations 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.

b. *No Carrier Sense*. Stations cannot sense the channel before trying to use it. They just go ahead and transmit. Only later can they determine whether the transmission was successful.

- ***Advantages***
    - ✓ Dynamic channel allocation schemes allot channels as needed. This results in optimum utilization of network resources.

- ✓ There are less chances of denial of services and call blocking in case of voice transmission.
- ✓ These schemes adjust bandwidth allotment according to traffic volume, and so are particularly suitable for bursty traffic.

- ***Disadvantages***
  - ✓ Dynamic channel allocation schemes increase the computational as well as storage load on the system.

2.3 Multiple Access Protocol

The data can be transmitted between the sender and receiver using a communication link. The data communication can be done at any time without any collision by establishing aedicated link between the sender and receiver. If we provide the dedicated link, the world is full of communication medium and not possible to create a dedicated link for any sender to any receiver. To avoid this problem, multiple users are allowed to access the single communication medium. By allowing multi user access, two or more users can try to access the communication medium at the same time. It leads to collision in the communication medium.

Hence the data link layer provides algorithm to share the communication medium and called as multiple access protocol. It means, a protocol allows multiple users to access a communication medium. The *Figure 2.9* illustrates the different categories of multiple access protocol used in data link layer.

In this chapter, we are studying random access protocols such as Aloha, CSMA, CSMA/CD, CSMA/CA.

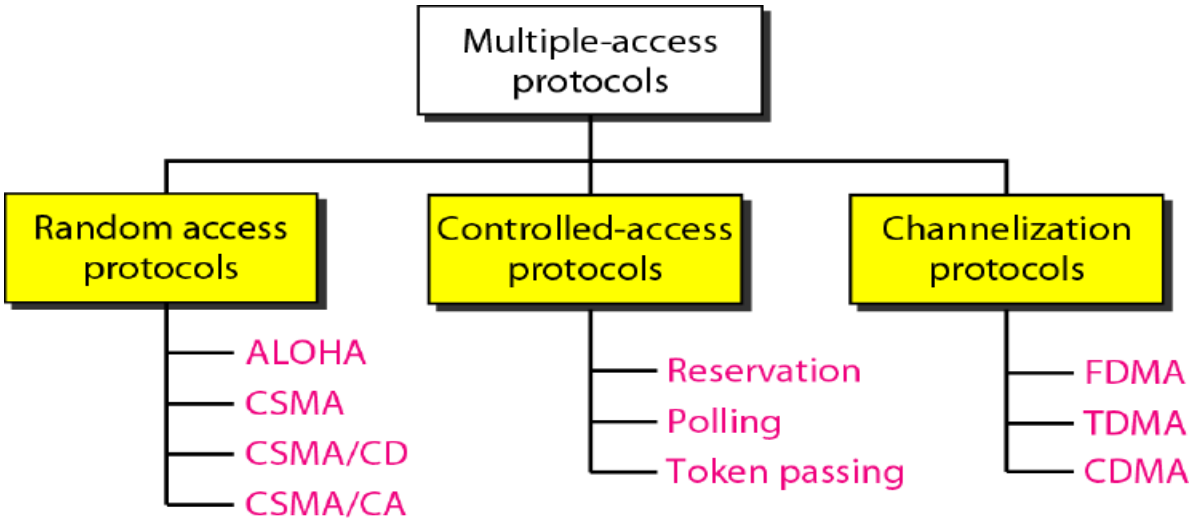


Figure :Types of Multiple Access Protocol

2.3.1ALOHA

ALOHA is a system proposed for solving the channel allocation problem. It is used for ground-based radio broadcasting. The basic idea is applicable to any system in which

uncoordinated users are competing for the use of a single shared channel. there are two versions of ALOHA:

a) Pure ALOHA
b) Slotted ALOHA

The basic difference with respect to timing is synchronization. The Pure ALOHA does not require global time synchronization, but, the Slotted ALOHA requires time synchronization.

Pure ALOHA

The pure ALOHA system is working as follows:

- ✓ let users transmit whenever they have data to be sent.
- ✓ expected collisions will occur.
- ✓ the collided frames will be destroyed.
- ✓ using a feedback mechanism to know about the status of frame.
- ✓ If the frame was destroyed, the sender just waits a random amount of time.
- ✓ retransmit the destroyed frame.

The waiting time must be random or the same frames will collide over and over, in lockstep. Systems in which multiple users share a common channel in a way that can lead to conflicts are widely known as contention systems.

A sketch of frame generation in a pure ALOHA and slotted ALOHA system is given in *Figure* a.

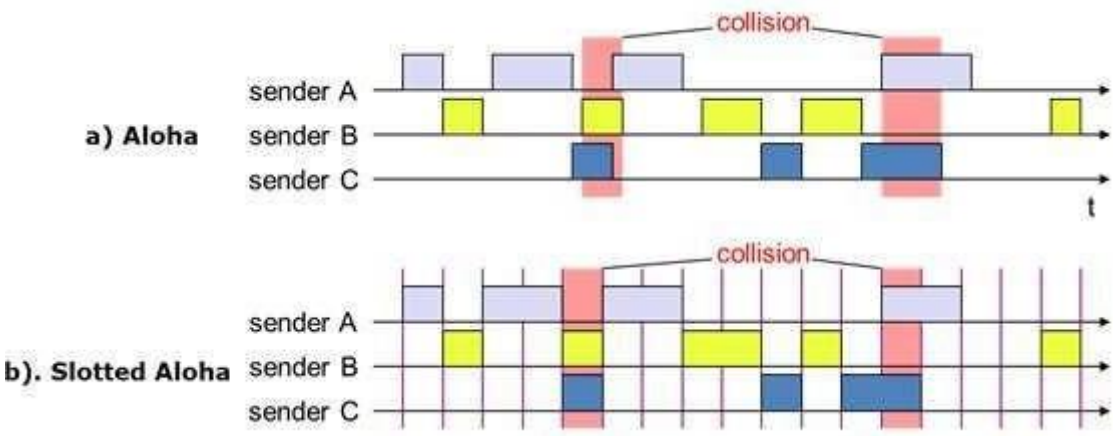


Figure: Aloha System for frame transmission

Whenever two frames try to occupy the channel at the same time, there will be a collision and both will be garbled. Even the first bit of a new frame overlaps with just the last bit of a frame almost finished, both frames will be totally destroyed and both will have to be retransmitted later.

- **Vulnerable time**

Let us find the length of time, the vulnerable time, in which there is a possibility of collision.

$$\text{Pure ALOHA vulnerable time} = 2 \times T_{fr}$$

Where T_{fr} is the frame transmission time.

- **Throughput**

Let us call G the average number of frames generated by the system during one frame transmission time.

$$\text{The throughput for pure ALOHA is } S = G \times e^{-2G}.$$

$$\text{The maximum throughput } S_{max} = 0.184 \text{ when } G = (1/2).$$

Slotted ALOHA

In slotted ALOHA, we divide the time into equal size slots and force the station to send only at the beginning of the time slot. The *Figure 2.10*.b shows the example of collision and successful transmission frame in slotted aloha.

Because a station is allowed to send only at the beginning of the synchronized time slot, if a station misses this moment, it must wait until the beginning of the next time slot. This means that the station which started at the beginning of this slot has already finished sending its frame.

$$\text{Slotted ALOHA vulnerable time} = T_{fr}$$

$$\text{The throughput for slotted ALOHA is } S =: G \times e^{-G}.$$

$$\text{The maximum throughput } S_{max} == 0.368 \text{ when } G=1.$$

The efficiency of pure ALOHA and slotted ALOHA is shown in Figure 2.11. The maximum throughput of pure ALOHA is 18% and slotted ALOHA is 37%.

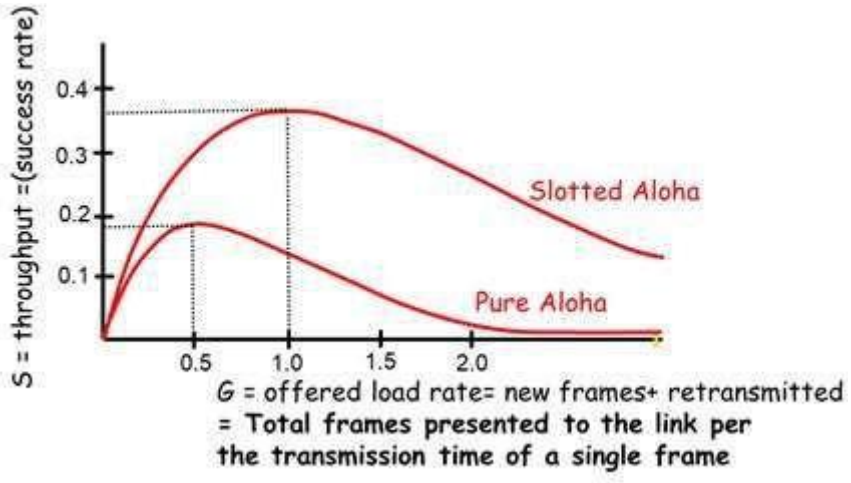


Figure : Efficiency of ALOHA methods

2.3.2 Carrier Sense Multiple Access (CSMA)

The CSMA protocol was developed to reduce the collision in multiple access. It is done by sensing the channel before transmitting by a station. If the channel is free, then the station can transmit; otherwise, the station must wait. In other words, CSMA is based on the principle "`sense before transmit`" or "`listen before talk`."

Even the CSMA reduces the collision, but it cannot eliminate the collision. The possibility of collision still exists because of propagation delay; when a station sends a frame, it still takes time (although very short) for the first bit to reach every station and for every station to sense it. The vulnerable time for CSMA is the propagation time *Tp*.

- Persistence Methods

The persistence methods are used to reduce the collisions and follows CSMA scheme. What should a station do if the channel is busy? What should a station do if the channel is idle? Three methods have been devised to answer these questions:

c) 1-persistent method,
d) nonpersistent method,
e) p-persistent method.

a). 1-persistent method

In this method, a station wishing to transmit listens to the medium and obeys the following rules

1. If the medium is idle, transmit; otherwise, go to step 2.
2. If the medium is busy, continue to listen until the channel is sensed idle; then transmit immediately.

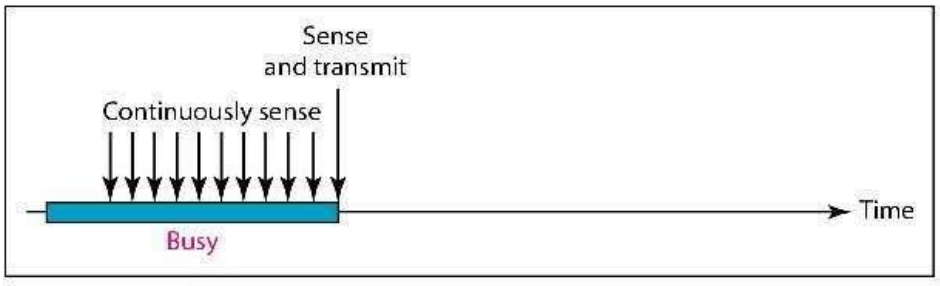


Figure : 1-Persistence Scheme

- Performance

The 1-persistent stations are selfish. If two or more stations becomes ready at the same time, collision guaranteed.

b). Nonpersistent method

In nonpersistent method, A station with frames to be sent, should sense the medium and do the follows.

1. If medium is idle, transmit; otherwise, go to 2
2. If medium is busy, (backoff) wait a random amount of time and repeat 1.

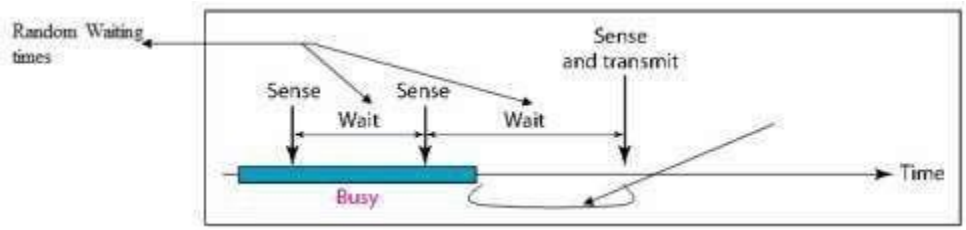


Figure: Non-persistent Scheme

- Performance

✓ Non-persistent Stations are deferential (respect others).

✓ Random delays reduce probability of collisions because two stations with data to be transmitted will wait for different amount of times.

✓ Bandwidth is wasted if waiting time (backoff) is large because medium will remain idle following end of transmission even if one or more stations have frames to send

c). p-persistent method

Time is divided to slots where each Time unit (slot) typically equals maximum propagation delay. In p-persistent method (shown in Figure 2.14), if a station wishing to transmit listens to the medium, it follows the following steps:

1. If medium idle,
   - ✓ transmit with probability (p), OR
   - ✓ wait one-time unit (slot) with probability (1 – p), then repeat 1.
2. If medium busy, continuously listen until idle and repeat step 1

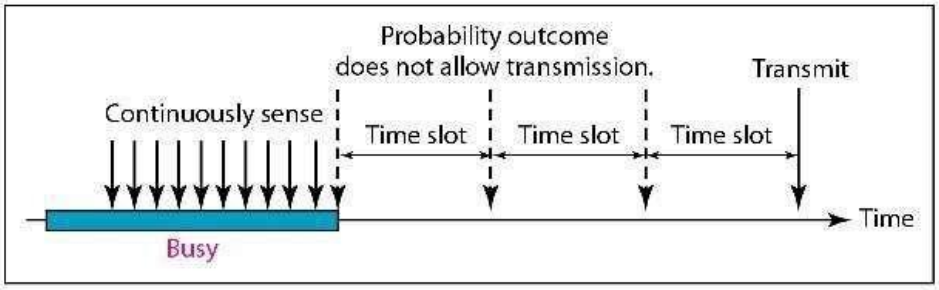


Figure : p-persistent scheme

- Performance:
  - ✓ Reduces the possibility of collisions like nonpersistent.
  - ✓ Reduces channel idle time like 1-persistent.

2.3.3 Carrier Sense Multiple Access with Collision Detection (CSMA/CD)

Carrier Sense Multiple Access with Collision Detection (CSMA/CD) is a network protocol for carrier transmission that operates in the Medium Access Control (MAC) layer. CSMA/CD (CSMA with Collision Detection) is widely used on LANs in the MAC sublayer. In particular, it is the basis of the popular Ethernet LAN.

CSMA/CD\uses the conceptual model of *Figure* . At the point marked t_0, a station has finished transmitting its frame. Any other station having a frame to send may now attempt to do so. If two or more stations decide to transmit simultaneously, there will be a collision. Collisions can be detected by looking at the power or pulse width of the received signal and comparing it to the transmitted signal.

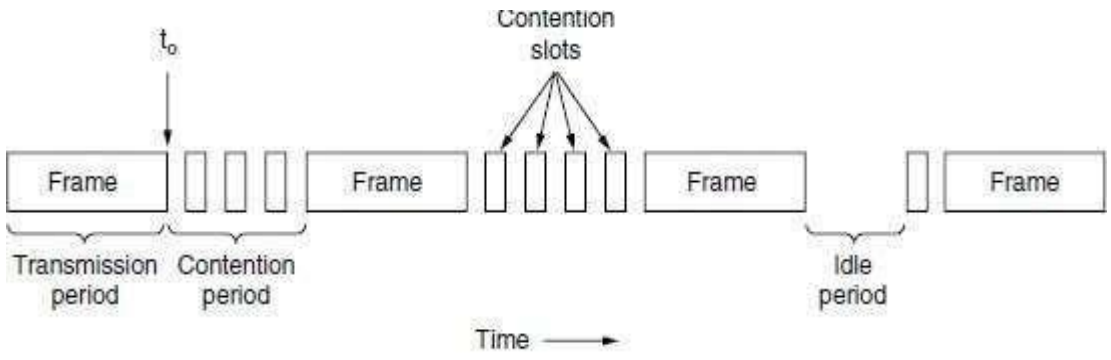


Figure :Transmission, Contention and idle states of CSMA/CD

The collision detection technology detects collisions by sensing transmissions from other stations. On detection of a collision, the station stops transmitting, sends a jam signal, and then waits for a random time interval before retransmission.

- **Algorithms**

The algorithm of CSMA/CD is:

1. When a frame is ready, the transmitting station checks whether the channel is idle or busy.
2. If the channel is busy, the station waits until the channel becomes idle.
3. If the channel is idle, the station starts transmitting and continually monitors the channel to detect collision.
4. If a collision is detected, the station starts the collision resolution algorithm.
5. The station resets the retransmission counters and completes frame transmission. The algorithm of Collision Resolution is:

1. The station continues transmission of the current frame for a specified time along with a jam signal, to ensure that all the other stations detect collision.

   The jam signal is a signal that carries a 32-bit binary pattern sent by a data station to inform the other stations that they must not transmit.
2. The station increments the retransmission counter.
3. If the maximum number of retransmission attempts is reached, then the station aborts transmission.
4. Otherwise, the station waits for a backoff period which is generally a function of the number of collisions and restart main algorithm.

Though the CSMA/CD algorithm detects collisions, it does not reduce the number of collisions. It is not appropriate for large networks performance degrades exponentially when more stations are added.

2.4Ethernet

Ethernet is a technology for connecting Local Area Networks. It is also known as IEEE 802.3. The architecture of Ethernet is shown in Figure 2.16.

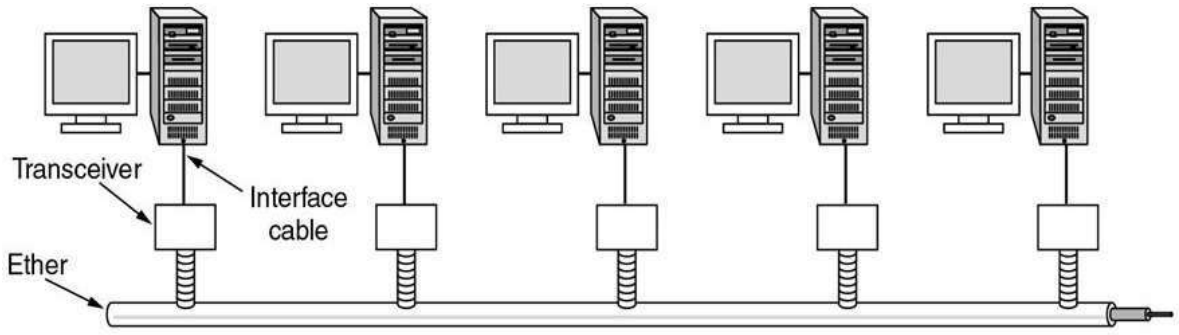


Figure : Architecture of Ethernet

Ethernet was the first Local Area Network (LAN) technology and remains the most important one. It was developed during the early 1970s by Xerox PARC. The original Ethernet enabled computers located within a few hundred yards of one another to exchange messages. By adding repeaters and bridges between multiple LANs, that distance has been extended to a few thousand yards. Thus, it is suitable for connecting the computers in a building or campus.

Ethernet architecture is based on the concept of connecting multiple computers to a long cable, sometimes called the ***ether***, thereby forming a bus structure. Each computer is fitted with an Ethernet adapter that includes a unique 48-bit address for that computer. Each computer is joined to the ether through a ***transceiver*** that forms a logical "T." The transceiver receives Ethernet messages on the cable, looks at the address, and either passes the message to its computer, if the address matches, or transmits it down the cable, if the address does not match.

2.4.1 Ethernet Cabling

The name "Ethernet" refers to the cable (the ether). Four types of cabling are commonly used,

- **10Base5** is called thick Ethernet. Connections use vampire taps. The first number, 10, is the speed in Mbps. The word "Base" (or sometimes "BASE") to indicate baseband transmission and can support segments of up to 500 meters (for coaxial cable).
- **10Base2** is called thin Ethernet. Connections are done using T junctions. This is cheaper and easier to install. But it can run for only 185 meters per segment, each of which can handle only 30 machines.

Detecting cable breaks, excessive length, bad taps, or loose connectors can be a major problem with both media. For this reason, techniques have been developed to track them down. Basically, a pulse of known shape is injected into the cable. If the pulse hits an obstacle or the end of the cable, an echo will be generated and sent back. By carefully timing the interval between sending the pulse and receiving the echo, it is possible to localize the origin of the echo. This technique is called ***time domain reflectometry***.

- **10BaseT** uses twisted pair cable and a hub. All stations have a cable running to a central hub.

Name	Cable	Max. seg.	Nodes/seg.	Advantages
10Base5	Thick coax	500 m	100	Original cable; now obsolete
10Base2	Thin coax	185 m	30	No hub needed
10Base-T	Twisted pair	100 m	1024	Cheapest system
10Base-F	Fiber optics	2000 m	1024	Best between buildings

Figure : Most Common kinds of Ethernet Cabling

- **10BaseF** uses fiber optics. This type is expensive due to the cost of connectors and terminators. It offers good security since wiretapping fiber is difficult.

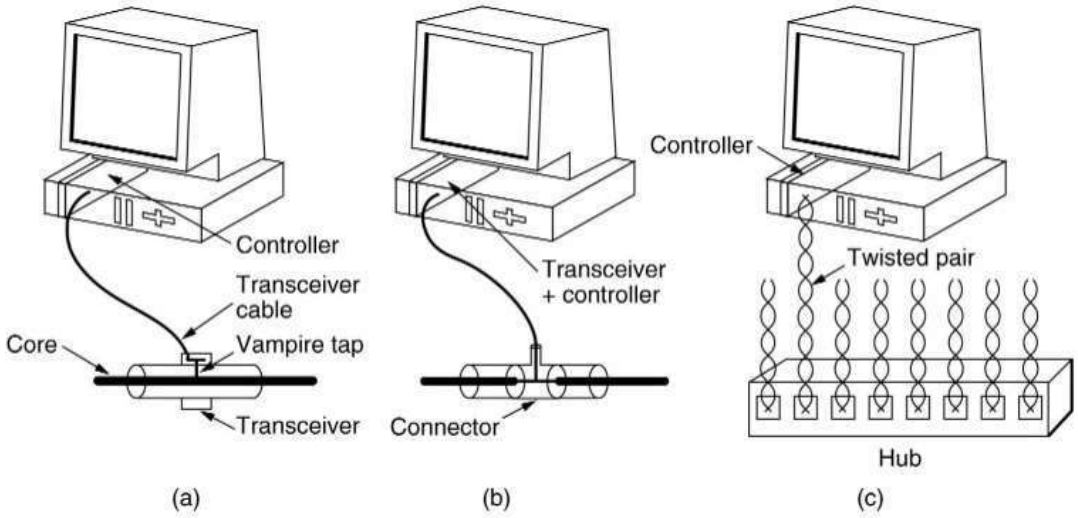


Figure: Three kinds of Ethernet cabling. (a) 10Base5. (b) 10Base2. (c) 10Base-T.

The major three wiring schemes are illustrated in Figure 2.18. For 10Base5, a transceiver is clamped securely around the cable so that its tap makes contact with the inner core. The transceiver contains the electronics that handle carrier detection and collision detection. When a collision is detected, the transceiver also puts a special invalid signal on the cable to ensure that all other transceivers also realize that a collision has occurred.

Different ways of wiring a building are shown in :

a. A single cable is snaked from room to room
b. A vertical spine runs from the basement to roof. Horizontal cables on each floor are connected to the spine.
c. Tree is the most general topology. Network with two paths between pairs of stations would suffer interference.

d. To allow large networks, multiple cables are connected by repeaters. A repeater received, amplifies and retransmits signals in both directions.

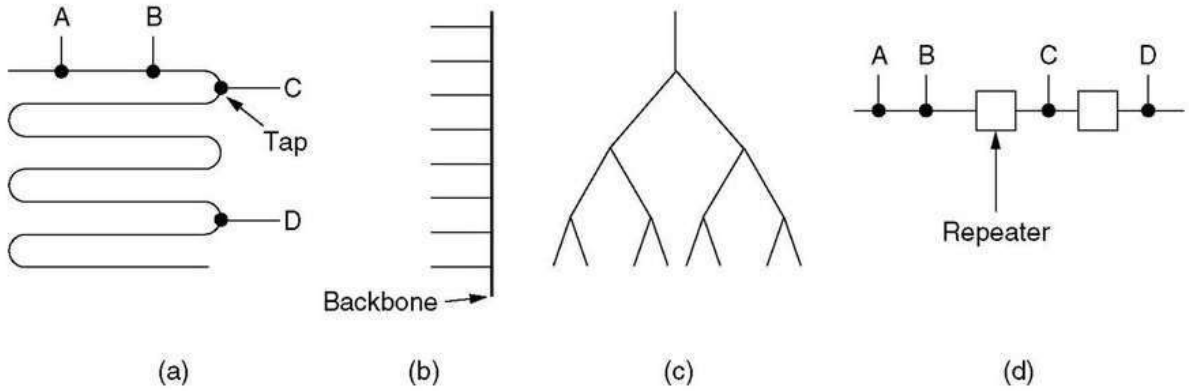


Figure: Cable topologies. (a) Linear. (b) Spine. (c) Tree. (d) Segmented

A **repeater** is a physical layer device. It receives, amplifies (regenerates), and retransmits signals in both directions. As far as the software is concerned, a series of cable segments connected by repeaters is no different from a single cable (except for some delay introduced by the repeaters). A system may contain multiple cable segments and multiple repeaters, but no two transceivers may be more than 2.5 km apart and no path between any two transceivers may traverse more than four repeaters.

2.4.2 Manchester Encoding

Binary encoding (Figure 2.20.a) uses only one voltage level, i.e positive voltage to represent binary 1 and zero voltage to represent binary 0. But, they cannot tell the difference between an idle sender (0 volts) and a 0 bit (0 volts). This problem can be solved by using +1 volts for a 1 and -1 volts for a 0. But still problem exists to identify the boundaries of bits, especially after a long run of consecutive 0s or a long run of consecutive 1s.

The above problem is solved in Manchester encoding and differential Manchester encoding. In Manchester encoding (Figure 2.20.b), a negative-to-positive transition represents bit 1 and a positive-to-negative transition represents binary 0.

In Differential Manchester, a transition means binary 0 and no transition means binary 1.

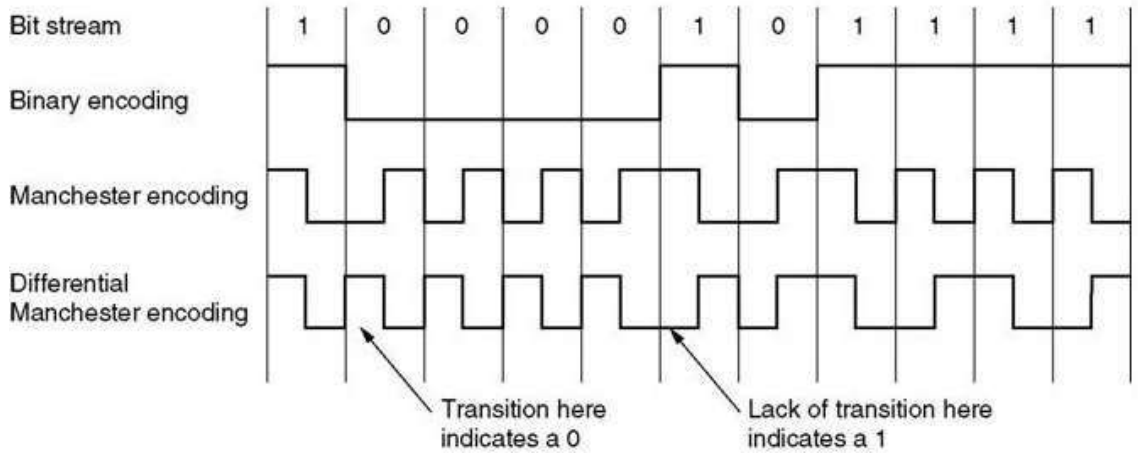


Figure : (a) Binary encoding. (b) Manchester encoding. (c) Differential Manchester encoding.

2.4.3 The Ethernet MAC Sublayer Protocol

a). DIX (DEC, Intel, Xerox) frame structure

Each frame starts with a *Preamble* of 8 bytes. It is used to keep track of frame boundaries. The frame contains two addresses: *destination* and *source address*. The higher order bit of destination address is 0 for ordinary addresses and 1 for group addresses. When a frame is sent to group address, all stations in the group receive it. This is called *multicasting*. If the frame is received by all the stations it is called *broadcasting*.

Type field tells the receiver what to do with the frame, which process to give the frame to. Next come the *data*, up to 1500 bytes. If the data portion is less than 46 bytes, the *Pad* field is used to fill the remaining space. The final field is the *checksum*, to check if error has occurred.

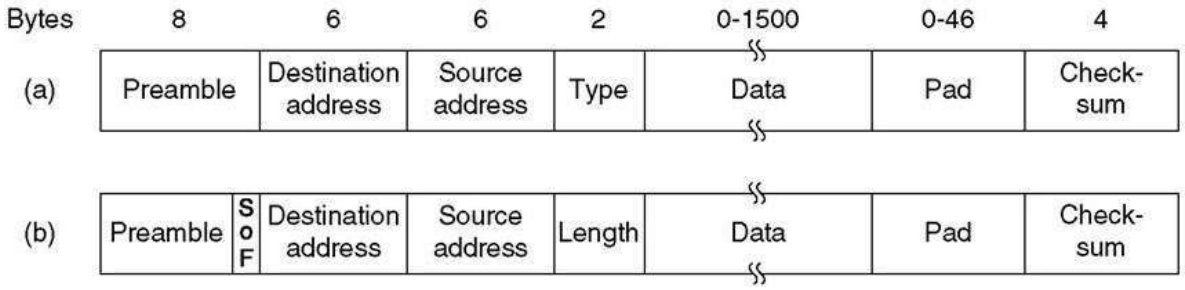


Figure :Ethernet Frame formats. (a) DIX Ethernet. (b) IEEE 802.3.

IEEE 802.3 frame structure

The *Preamble* is only 7 bytes long, and the 8th byte is for *Start of Frame* (SoF). The *Type* field is changed to *Length* field and the other fields remain the same as in DIX Ethernet frame format.

2.4.4 Binary Exponential Backoff Algorithm

After the first collision, each station waits either 0 or 1 slot times before trying again. If two stations collide, and each picks the same random number, they will collide again. After second collision, the station picks 0,1,2 or 3 at random, and waits for that number of slots. In general, the station waits at random from interval 0 to $2^i - 1$. The randomization interval grows exponentially.

This algorithm, called binary exponential backoff, was chosen to adapt dynamically adapt to the number of stations trying to send. If few stations collide, this algorithm causes low delay. If many number of stations collide, the collision is resolved in a reasonable interval of time.

2.4.5 Switched Ethernet

As more and more stations are added to Ethernet, the traffic will go up To deal with increased load, Switched Ethernet is used. The heart of this system is a ***switch***, containing 4 to 32 plug-in line cards, each containing one to eight connectors. Each connector has a 10BaseT twisted pair connection to a host computer.

When a station wants to transmit a frame, it outputs the frame to the switch. The plug-in card checks if the destination is in the same card. If so, frame is copied there. If not, the frame is sent to the backplane to the destination's card. Collision detection is done using CSMA/CD. As in the Figure 2.22, the port can be connected to a single station or to a *hub*.

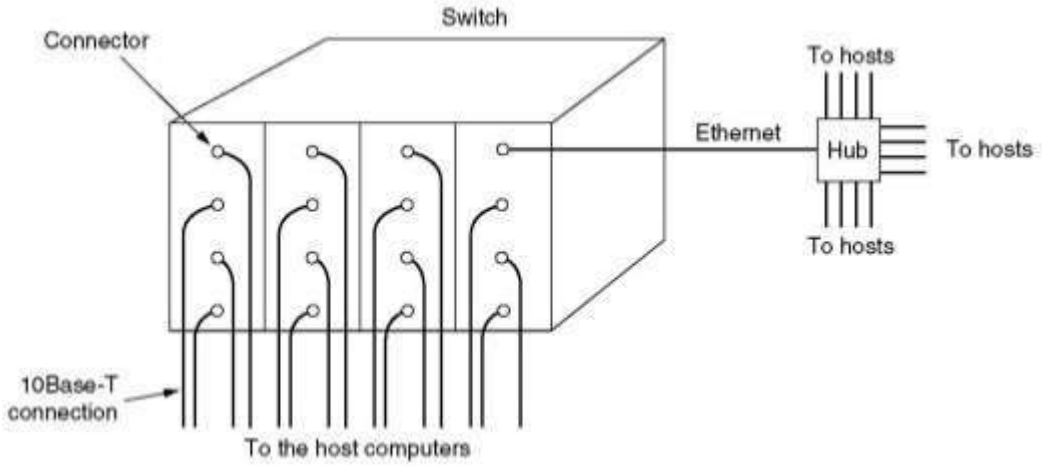


Figure : Simple Example of Switched Ethernet

2.4.6 Fast Ethernet

Fast Ethernet was designed to compete with LAN protocols such as FDDI or Fiber Channel (or Fibre Channel, as it is sometimes spelled). IEEE created Fast Ethernet under the name 802.3u. Fast Ethernet is backward-compatible with Standard Ethernet, but it can transmit data 10 times faster at a rate of 100 Mbps. The goals of Fast Ethernet can be summarized as follows:

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.

It reduces the bit time from 100 nsec to 10 nsec. All Fast Ethernets use hubs and switches. Ethernet cabling used is as follows and shown in Figure 2.23:

- 100Base-T4, used a signaling speed of 25 MHz, only 25% faster than standard Ethernets. It uses category 3 cable.
- 100Base-T4 requires four twisted pairs. Of the four pairs, one is always to the hub, one is always from the hub, and the other two are switchable to the current transmission direction.
- 100Base-TX Ethernet design is simpler because the wires can handle clock rates of 125 MHz. Only two twisted pairs per station are used, one to the hub and one from it. The 100Base-TX system is full duplex Stations can transmit at 100 Mbps on one twisted pair and receive at 100 Mbps on another twisted pair at the same time.
- 100Base-FX, uses two strands of multimode fiber, one for each direction, so it, too, can run full duplex with 100 Mbps in each direction. In this setup, the distance between a station and the switch can be up to 2 km.

Name	Cable	Max. segment	Advantages
100Base-T4	Twisted pair	100 m	Uses category 3 UTP
100Base-TX	Twisted pair	100 m	Full duplex at 100 Mbps
100Base-FX	Fiber optics	2000 m	Full duplex at 100 Mbps; long runs

Figure :The original fast Ethernet cabling

2.4.7 Gigabit Ethernet

All configurations of Gigabit Ethernet (IEEE 802.3z) use point-to-point links. The need for an even higher data rate resulted in the design of the Gigabit Ethernet protocol (1000 Mbps). The IEEE committee calls the Standard 802.3z. The goals of the Gigabit Ethernet design can be summarized as follows:

1. Upgrade the data rate to 1 Gbps.
2. Make it compatible with Standard or Fast Ethernet.
3. Use the same 48-bit address.
4. Use the same frame format.
5. Keep the same minimum and maximum frame lengths.
6. To support auto-negotiation as defined in Fast Ethernet.

In the simplest configuration, illustrated in Figure (a), two computers are directly connected to each other. The more common case, however, uses a switch or a hub connected to multiple computers and possibly additional switches or hubs, as shown in Figure(b).

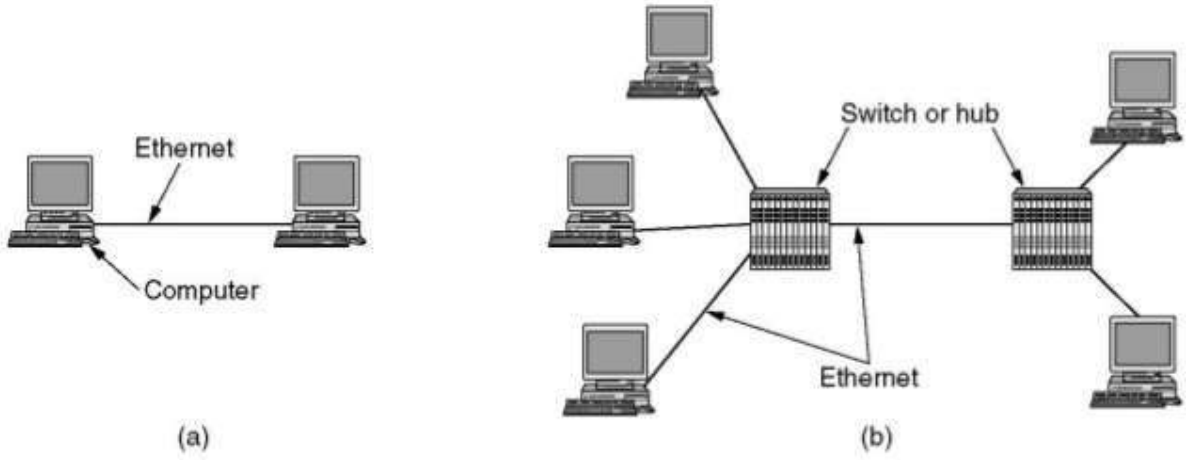


Figure: (a) A two-station Ethernet. (b) A multistation Ethernet

In both configurations, each individual Ethernet cable has exactly two devices on it, no more and no fewer. Gigabit Ethernet supports two different modes of operation: full-duplex mode and half-duplex mode.

The ‘‘normal’’ mode is *full duplex* mode, which allows traffic in both directions at the same time. This mode is used when there is a central switch connected to computers (or other switches) on the periphery.

The other mode of operation, *half-duplex*, is used when the computers are connected to a hub rather than a switch. In this mode, collisions are possible, so the standard CSMA/CD protocol is

required.

Gigabit Ethernet has two main features:

- The first feature, called carrier extension, essentially tells the hardware to add its own padding after the normal frame to extend the frame to 512 bytes.
- Since the second feature, called frame bursting, allows a sender to transmit a concatenated sequence of multiple frames in a single transmission

Gigabit Ethernet cabling is shown in figure.

Name	Cable	Max. segment	Advantages
1000Base-SX	Fiber optics	550 m	Multimode fiber (50, 62.5 microns)
1000Base-LX	Fiber optics	5000 m	Single (10 μ) or multimode (50, 62.5 μ)
1000Base-CX	2 Pairs of STP	25 m	Shielded twisted pair
1000Base-T	4 Pairs of UTP	100 m	Standard category 5 UTP

Figure : Original Gigabit Ethernet cabling

Gigabit Ethernet supports both copper and fiber cabling. To support 1Gbps, lasers are required as light source. Two wavelengths are permitted: 0.85 microns (Short) and 1.3 microns (Long). Lasers at 0.85 microns are cheaper but do not work on single-mode fiber.

Three fiber diameters are permitted: 10, 50, and 62.5 microns. The first is for single mode and the last two are for multimode.

2.4.8 IEEE 802.2: Logical Link Control

It hides the differences between the various kinds of 802 networks by providing a single format and interface to the network layer. LLC forms the upper half of the data link layer, with the MAC sublayer below it, as shown in here.

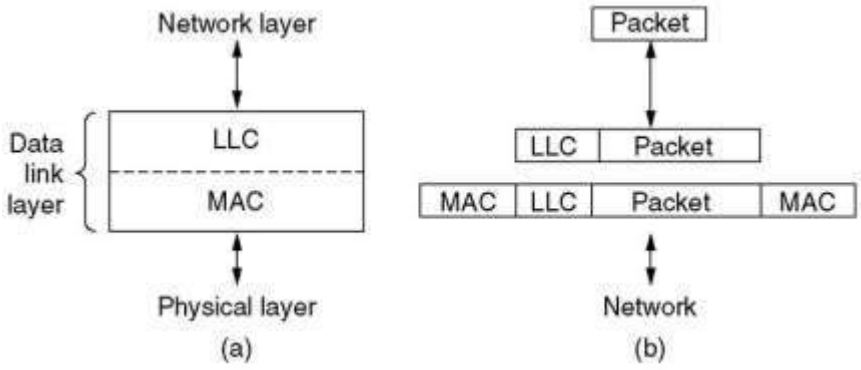


Figure : (a) Position of LLC. (b) Protocol formats

Network layer passes the packet to LLC. LLC adds an LLC header containing sequence and acknowledgement numbers. The header is attached to the payload. At the receiver, the reverse process takes place.

LLC provides three service options: a) Unreliable datagram service b)Acknowledged datagram service c)Reliable connection-oriented service. The LLC header has three fields: destination and source access points, and a control field. The control field contains sequence and acknowledgement numbers.

Retrospective on Ethernet

- ✓ Ethernet is simple and flexible.
- ✓ Ethernet is reliable, cheap, and easy to maintain.
- ✓ Thin Ethernet and twisted-pair wiring are relatively inexpensive
- ✓ Ethernet is easy to maintain.
- ✓ There is no software to install (other than the drivers) and not much in the way of configuration tables to manage.
- ✓ Adding new hosts is as simple as just plugging them in.
- ✓ Ethernet interworks easily with TCP/IPIP is a connectionless protocol, so it fits perfectly with Ethernet, which is also connectionless.
- ✓ Ethernet has been able to evolve in certain crucial ways.
- ✓ Speeds have gone up by several orders of magnitude; hubs and switches have been introduced.
- ✓ But these changes have not required changing the software and have often allowed the existing cabling to be reused for a time.

2.5 Wireless LAN

A wireless LAN (WLAN) is a wireless computer network that links two or more devices using wireless distribution method to form a local area network (LAN) within a limited area such as a home, school, computer laboratory, campus, office building etc. This gives users the ability to move around within the area and yet still be connected to the network (*Figure 2.27*).

Most modern WLANs are based on IEEE 802.11 standards and are marketed under the Wi-Fi brand name. Wireless LANs have become popular for use in the home, due to their ease of installation and use. They are also popular in commercial properties that offer wireless access to

their employees and customers.

Advantages of Wireless LANs

- ✓ ***Flexibility***: Within radio coverage, nodes can communicate without further restriction. Radio waves can penetrate walls, senders and receivers can be placed anywhere (also non-visible, e.g., within devices, in walls etc.).
- ✓ ***Planning***: Only wireless ad-hoc networks allow for communication without previous planning, any wired network needs wiring plans.

Figure: Example of Wireless LAN

Design:

Wireless networks allow for the design of independent, small devices which can for example be put into a pocket. Cables not only restrict users but also designers of small notepads, PDAs, etc.

✓ ***Robustness***: Wireless networks can handle disasters, e.g., earthquakes, flood etc. whereas, networks requiring a wired infrastructure will usually break down completely in disasters.

✓ ***Cost***: The cost of installing and maintaining a wireless LAN is on average lower than the cost of installing and maintaining a traditional wired LAN, for two reasons.

✓ ***Ease of Use***: Wireless LAN is easy to use and the users need very little new information to take advantage of WLANs.

Disadvantages of wireless LANs

✓ ***Quality of Services***: Quality of wireless LAN is typically lower than wired networks. The main reason for this is the lower bandwidth due to limitations is radio transmission, higher error rates due to interference and higher delay/delay variation due to extensive error correction and detection mechanisms.

✓ ***Proprietary Solutions***: Due to slow standardization procedures, many companies have come up with proprietary solutions offering standardization functionality plus many enhanced features. Most components today adhere to the basic standards IEEE 802.11a or 802.11b.

✓ ***Restrictions***: Several govt. and non-govt. institutions world-wide regulate the operation and restrict frequencies to minimize interference.

✓ ***Global operation***: Wireless LAN products are sold in all countries so, national and international frequency regulations have to be considered.

✓ ***Low Power***: Devices communicating via a wireless LAN are typically power consuming, also wireless devices running on battery power. Whereas the LAN design should take this into account and implement special power saving modes and power management functions.

✓ ***License free operation***: LAN operators don't want to apply for a special license to be able to use the product. The equipment must operate in a license free band, such as the
2.4 GHz ISM band.

✓ ***Robust transmission technology***: If wireless LAN uses radio transmission, many other electrical devices can interfere with them (such as vacuum cleaner, train engines, hair dryers, etc.). Wireless LAN transceivers cannot be adjusted for perfect transmission is a standard office or production environment.

2.6 The 802.11 Protocol Stack

The protocols used by all the 802 variants, including Ethernet, have a certain commonality of structure. A partial view of the 802.11 protocol stack is given in figure.

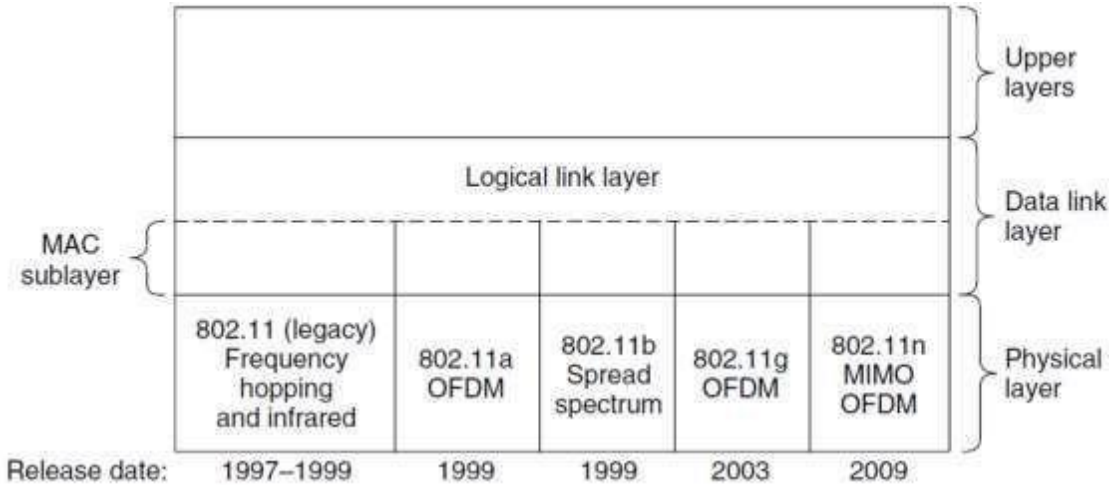


Figure : Protocol stack of 802.11

1. Physical Layer

The physical layer corresponds to the OSI physical layer fairly well. The following are the standards used in physical layer

- 802.11 Infrared (1997) – same technology as television remote controls do.
- 802.11 FHSS (1997) – used Frequency Hopping Spread Spectrum
- 802.11 DSSS (1997) – used Direct Sequence Spread Spectrum
  - Both FHSS and DSS does not require licensing (the 2.4-GHz ISM band).
  - Operate at 1 or 2 Mbps and at low enough power that they do not conflict too much.
  - Example - Radio-controlled garage door openers, Cordless telephones and microwave ovens
- 802.11a OFDM (1999) – used Orthogonal Frequency Division Multiplexing technique and operate at up to 54 Mbps.
- 802.11b HR-DSSS (1999) – used High Rate DSSS technique and operate at up to 11 Mbps.
- 802.11g OFDM (2001) – used OFDM modulation, but, different frequency band from OFDM.

2. Data Link Layer (DLL)

The data link layer in all the 802 protocols is split into two or more sublayers. In 802.11, the MAC (Medium Access Control) sublayer determines how the channel is allocated, that is, who gets to transmit next. Above it is the LLC (Logical Link Control) sublayer, whose job it is to hide the

differences between the different 802 variants and make them indistinguishable as far as the network layer is concerned.

2.6.1 The 802.11 Physical Layer

Each of the five permitted transmission techniques makes it possible to send a MAC frame from one station to another.

1. ***Infrared***

   - ✓ uses diffused (i.e., not line of sight) transmission at 0.85 or 0.95 microns.
   - ✓ Two capacities 1 Mbps (4-bit encoding produced 16-bit codeword) or 2 Mbps (2-bit encoding produced 4-bit codeword).
   - ✓ Range is 10 to 20 meters and cannot penetrate walls.
   - ✓ Does not work outdoors.

2. ***FHSS***

   - ✓ The main issue is multipath fading.
   - ✓ 79 non-overlapping channels, each 1 MHz wide at low end of 2.4 GHz ISM band.
   - ✓ Same pseudo-random number generator used by all stations.
   - ✓ Dwell time: min. time on channel before hopping (400msec).
   - ✓ Its main disadvantage is its low bandwidth.

3. ***DSSS***

   - ✓ Spreads signal over entire spectrum using pseudo-random sequence (similar to CDMA).
   - ✓ Each bit transmitted using an 11 chips Barker sequence, PSK at 1Mbaud.
   - ✓ Operates at 1 or 2 Mbps.

4. ***OFDM***

   - ✓ Compatible with European HiperLan2.
   - ✓ 54Mbps in wider 5.5 GHz band - transmission range is limited.
   - ✓ Uses 52 FDM channels (48 for data; 4 for synchronization).
   - ✓ Encoding is complex (PSM up to 18 Mbps and QAM above this capacity).
   - ✓ E.g., at 54Mbps 216 data bits encoded into 288-bit symbols.
   - ✓ More difficulty penetrating walls.

5. ***HR-DSSS***

- ✓ 11a and 11b shows a split in the standards committee.
- ✓ 11b approved and hit the market before 11a.
- ✓ Up to 11 Mbps in 2.4 GHz band using 11 million chips/sec.
- ✓ Note in this bandwidth all these protocols have to deal with interference from microwave ovens, cordless phones and garage door openers.
- ✓ Range is 7 times greater than 11a.
- ✓ 11b and 11a are incompatible!!

2.6.2 The 802.11 MAC Sublayer Protocol

The 802.11 MAC sublayer provides an abstraction of the physical layer to the logical link control sublayer and upper layers of the OSI network. It is responsible for encapsulating frames and describing frame formats.

MAC layer provides functionality for several tasks like control medium access, can also offer support for roaming, authentication, and power conservation. The basic services provided by MAC are the mandatory asynchronous data service and an optional time-bounded service.

IEEE 802.11 defines two MAC sub-layers :

1. Distributed Coordination Function (DCF) - DCF uses CSMA/CD as access method as wireless LAN can't implement CSMA/CD. It only offers asynchronous service.
2. Point Coordination Function (PCF) - PCP is implemented on top of DCF and mostly used for time-service transmission. It uses a centralized, contention-free polling access method. It offers both asynchronous and time-bounded service.

- **Avoidance of Collisions by 802.11 MAC Sublayer**

In wireless systems, the method of collision detection does not work. It uses a protocol called carrier sense multiple access with collision avoidance (CSMA/CA).

The method of CSMA/CA is

- ✓ When a frame is ready, the transmitting station checks whether the channel is idle or busy.
- ✓ If the channel is busy, the station waits until the channel becomes idle.
- ✓ If the channel is idle, the station waits for an Inter-frame gap (IFG) amount of time and then sends the frame.
- ✓ After sending the frame, it sets a timer.

✓ The station then waits for acknowledgement from the receiver. If it receives the acknowledgement before expiry of timer, it marks a successful transmission.

✓ Otherwise, it waits for a back-off time period and restarts the algorithm.

2.6.3 The 802.11 Frame Structure

The 802.11 standard defines three different classes of frames on the wire: data, control, and management. Each of these has a header with a variety of fields used within the MAC sublayer.

The MAC layer frame consists of 9 fields. The Figure 2.29 shows the basic structure of an IEEE 802.11 MAC data frame along with the content of the frame control field.

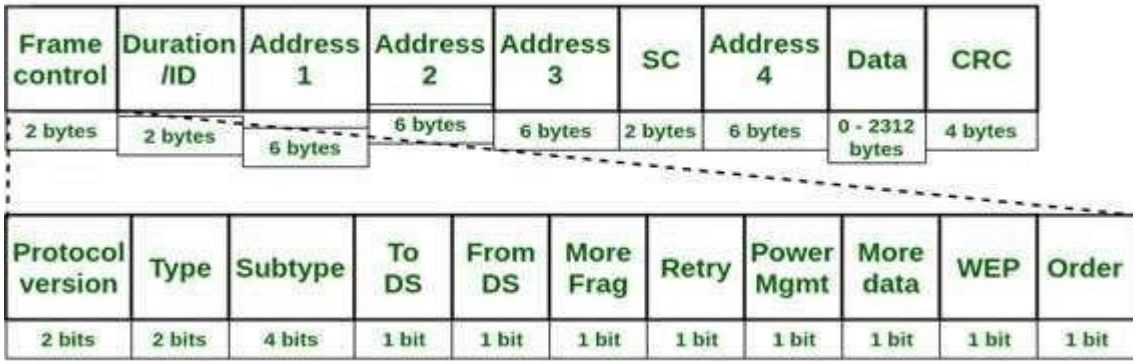


Figure :The 802.11 MAC Frame Structure

- ***Frame Control(FC)*** - It is 2 bytes long field which defines type of frame and some control information. Various fields present in FC are:

1)Version - It is a 2 bit long field which indicates the current protocol version which is fixed to be 0 for now.

2)Type - It is a 2 bit long field which determines the function of frame i.e management(00), control(01) or data(10). The value 11 is reserved.

3)Subtype - It is a 4 bit long field which indicates sub-type of the frame like 0000 for association request, 1000 for beacon.

4)To DS - It is a 1 bit long field which when set indicates that destination frame is for DS(distribution system).

5)From DS - It is a 1 bit long field which when set indicates frame coming from DS.

6)More frag (More fragments) - It is 1 bit long field which when set to 1 means frame is followed by other fragments.

7)Retry -It is 1 bit long field, if the current frame is a retransmission of an earlier frame, this

bit is set to 1.

8)Power Mgmt (Power management) - It is 1 bit long field which indicates the mode of a station after successful transmission of a frame. Set to 1 the field indicates that the station goes into power-save mode. If the field is set to 0, the station stays active.

9)More data - It is 1 bit long field which is used to indicates a receiver that a sender has more data to send than the current frame. This can be used by an access point to indicate to a station in power-save mode that more packets are buffered or it can be used by a station to indicate to an access point after being polled that more polling is necessary as the station has more data ready to transmit.

10) WEP - It is 1 bit long field which indicates that the standard security mechanism of 802.11 is applied.

11) Order - It is 1 bit long field, if this bit is set to 1 the received frames must be processed in strict order.

- ***Duration*** − It is a 2-byte field that specifies the time period for which the frame and its acknowledgement occupy the channel.
- ***Address fields*** − There are three 6-byte address fields containing addresses of source, immediate destination and final endpoint respectively.
- ***Sequence*** − It a 2 bytes field that stores the frame numbers.
- ***Data*** − This is a variable sized field carries the data from the upper layers. The maximum size of data field is 2312 bytes.
- ***Check Sequence*** − It is a 4-byte field containing error detection information.

Services

The 802.11 standard defines the services that the clients, the access points, and the network connecting them must be a conformant wireless LAN. These services are divided into two categories: five distribution services and four station services. The distribution services relate to managing cell membership and interacting with stations outside the cell.

a. Distribution Services

The five distribution services are provided by the base stations and deal with station mobility as they enter and leave cells, attaching themselves to and detaching themselves from base stations. They are as follows.

1. ***Association***. This service is used by mobile stations to connect themselves to base stations. Typically, it is used just after a station moves within the radio range of the base station. Upon arrival, it announces its identity and capabilities. The capabilities include the data rates supported, need for PCF services (i.e., polling), and power management requirements. The base station may accept or reject the mobile station. If the mobile station is accepted, it must then authenticate itself.

2. ***Disassociation***. Either the station or the base station may disassociate, thus breaking the relationship. A station should use this service before shutting down or leaving, but the base station may also use it before going down for maintenance.

3. ***Reassociation***. A station may change its preferred base station using this service. This facility is useful for mobile stations moving from one cell to another. If it is used correctly, no data will be lost as a consequence of the handover. (But 802.11, like Ethernet, is just a best-efforts service.)

4. ***Distribution***. This service determines how to route frames sent to the base station. If the destination is local to the base station, the frames can be sent out directly over the air. Otherwise, they will have to be forwarded over the wired network.

5. ***Integration***. If a frame needs to be sent through a non-802.11 network with a different addressing scheme or frame format, this service handles the translation from the 802.11 format to the format required by the destination network.

b. Station Services

The remaining four services are intracell (i.e., relate to actions within a single cell). They are used after association has taken place and are as follows.

1. ***Authentication***. Because wireless communication can easily be sent or received by unauthorized stations, a station must authenticate itself before it is permitted to send data by challenge and response method. If the result is correct, the mobile is fully enrolled in the cell.

2. ***Deauthentication***. When a previously authenticated station wants to leave the network, it is deauthenticated. After deauthentication, it may no longer use the network.

3. ***Privacy***. For information sent over a wireless LAN to be kept confidential, it must be encrypted. This service manages the encryption and decryption. The encryption algorithm specified is RC4.

4. ***Data delivery***. Finally, data transmission is what it is all about, so 802.11 naturally provides a way to transmit and receive data. Transmission over 802.11 is not guaranteed

to be reliable. Higher layers must deal with detecting and correcting errors.

2.6.4 IEEE 802.11 Architecture

The IEEE 802.11 standard defines the physical layer and media access control (MAC) layer for a wireless local area network. The standard defines three different physical layers for the 802.11 wireless LAN, each operating in a different frequency range and at rates of 1 Mbps and 2 Mbps.

Modes of Wireless LAN

802.11 networks can be used in two modes:

- Infrastructure mode
- Ad-hoc mode

- ***Infrastructure mode***

In infrastructure mode (Figure 2.30), each client is associated with an AP (Access Point) that is in turn connected to the other network. The client sends and receives its packets via the AP. Several access points may be connected together, typically by a wired network called a distribution system, to form an extended 802.11 network. In this case, clients can send frames to other clients via their APs.

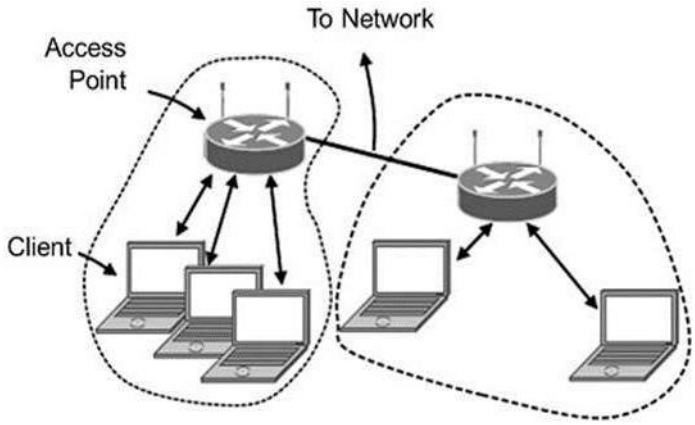


Figure : Infrastructure Mode

The most popular mode is to connect clients, such as laptops and smart phones, to another network, such as a company intranet or the Internet.

- ***Ad-hoc mode***

The other mode is an ad hoc network. This mode is a collection of computers that are associated so that they can directly send frames to each other. There is no access point. Since Internet access is

the killer application for wireless, ad hoc networks are not very popular.

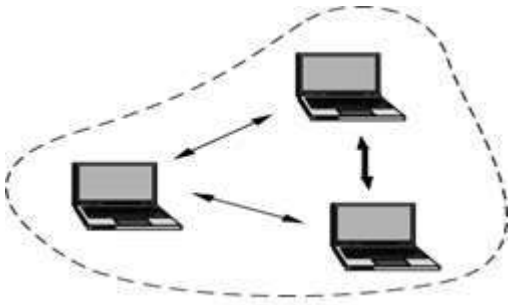


Figure : Ad-hoc Mode

Service Model

The standard defines two kinds of services: the basic service set (BSS) and the extended service set (ESS).

- ***Basic Service Set***

IEEE 802.11 defines the basic service set (BSS) as the building block of a wireless LAN. A basic service set is made of stationary or mobile wireless stations and an optional central base station, known as the access point (AP). Figure 2.32 shows two sets in this standard.

The BSS without an AP is a stand-alone network and cannot send data to other BSSs. It is called an ad hoc architecture. In this architecture, stations can form a network without the need of an AP; they can locate one another and agree to be part of a BSS. A BSS with an AP is sometimes referred to as an infrastructure network.

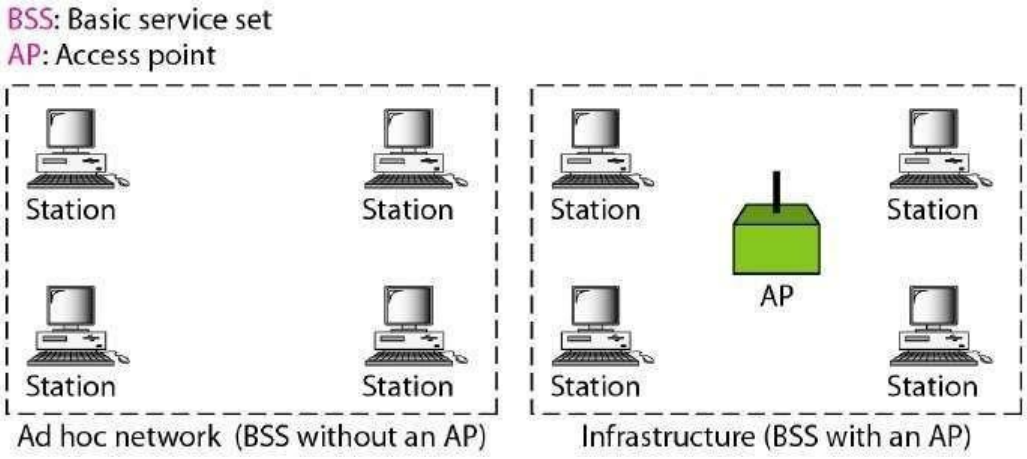


Figure Basic Service Set

Extended Service Set

An extended service set (ESS) is made up of two or more BSSs with APs. In this case, the BSSs are connected through a distribution system, which is usually a wired LAN. The distribution

system connects the APs in the BSSs. IEEE 802.11 does not restrict the distribution system; it can be any IEEE LAN such as an Ethernet. Note that the extended service set uses two types of stations: mobile and stationary. The mobile stations are normal stations inside a BSS. The stationary stations are AP stations that are part of a wired LAN. Figure 2.33 shows an ESS.

When BSSs are connected, the stations within reach of one another can communicate without the use of an AP. However, communication between two stations in two different BSSs usually occurs via two APs. The idea is similar to communication in a cellular network if we consider each BSS to be a cell and each AP to be a base station. Note that a mobile station can belong to more than one BSS at the same time.

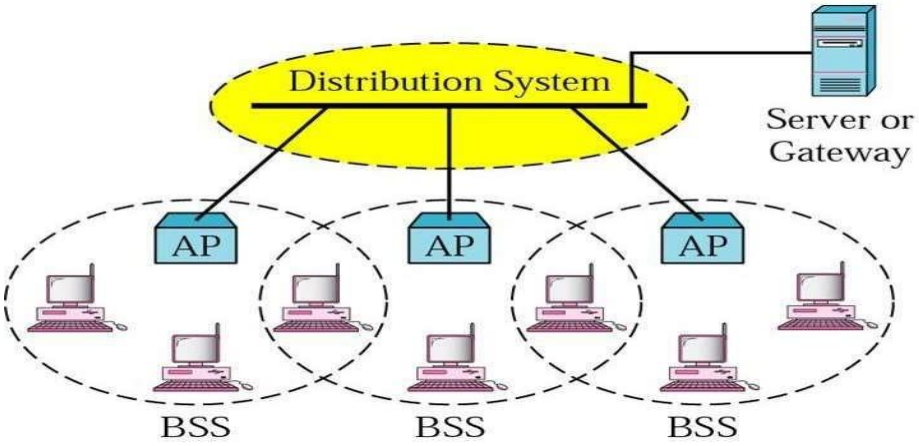


Figure: Extended Service Set

Short Questions and Answers

1. What is meant by Data Link Layer(DLL)?

The Data Link Layer is the second layer in the OSI model, above the Physical Layer, which ensures that the error free data is transferred between the adjacent nodes in the network.

2. What are the functions included in Data Link Layer in Design Issues?

- Providing a well-defined service interface to the network layer.
- Dealing with transmission errors.
- Regulating the flow of data so that slow receivers are not swamped by fast senders –flow control.

3. What are all the functions in data link control include?

(1) Framing.
(2) Error Control.
(3) Flow Control.

4. What **is** Framing**?**

It breaks the datagram passed down by above layers and converts them into frames ready for transfer. This is called **Framing.**

5. What are the three distinct phases?

1. Connection established
2. Frames are transmitted
3. Connection released

6. List out the framing Methods

1. Character count.
2. Flag bytes with byte stuffing.
3. Starting and ending flags, with bit stuffing.
4. Physical layer coding violations.

7. What is Fixed Size Framing?

In fixed-size framing, there is no need for defining the boundaries of the

frames. The size itself can be used as a delimiter.

8. Define Character Stuffing?

In byte stuffing (or character stuffing), a special byte is added to the data section of the frame when there is a character with the same pattern as the flag. The data section is stuffed with an extra byte. This byte is usually called the escape character (ESC), which has a predefined bit pattern. Whenever the receiver encounters the ESC character, it removes it from the data section and treats the next character as data, not a delimiting flag.

9. What is Bit Stuffing?

Bit stuffing is the process of adding one extra 0 whenever five consecutive 1s follow a 0 in the data, so that the receiver does not mistake the pattern 0111110 for a flag.

10. What is error Control?

Having solved the problem of marking the start and end of each frame and how to make sure all frames are eventually delivered to the network layer at the destination and inthe proper order.

11. Write any two disadvantage of Error Control

- If a frame vanishes, the receiver will not send an acknowledgement thus, sender will wait forever
- Sender transmits a frame , starts a Timer.

12. What are the approaches commonly used for Flow Control

    - feedback-based flow control
    - rate-based flow control

13. What is Network Interface card (NIC)?

A NIC is a component that provides networking capabilities for a computer. It may enable a wired connection (such as Ethernet)or a wireless connection(such as Wi-Fi) to a local area network.

14. How the network layer services have been designed?

    a. The services should be independent of the router technology.

b. The transport layer should be shielded from the number, type, and topology of the routers present.

c. The network addresses made available to the transport layer should use a uniform numbering plan, even across LANs and WANs.

15. Define Flow control.

Flow control is a technique that allows two stations working at different speeds to communicate with each other. It is a set of measures taken to regulate the amount of data that a sender sends so that a fast sender does not overwhelm a slow receiver.

16. What is meant by Channel Allocation?

A channel allocation is how to allocate a single broadcast channel among competing users. The allocation is divided into static and dynamic channel allocation.

17. Define static channel allocation.

In static channel allocation schemes, frequency channels are permanently allotted to any user.

18. Define dynamic channel allocation.

In dynamic channel allocation schemes, frequency channels are not permanently allotted to any user. Channels are assigned to the user as needed depending upon the network environment.

19. What is meant by Carrier Sense Multiple Access (CSMA)?

The CSMA protocol was developed to reduce the collision in multiple access. It is done by sensing the channel before transmitting by a station. If the channel is free, then the station can transmit; otherwise, the station must wait. In other words, CSMA is based on the principle "sense before transmit" or "listen before talk."

20. What is Jam Signal?

The jam signal is a signal that carries a 32-bit binary pattern sent by a data station to inform the other stations that they must not transmit.

21. What is Multiple Access?

If the physical links are shared by more than two nodes, it is said to be Multiple Access.

22. Define Datagrams?

The packets are frequently called datagrams (in analogy with telegrams).

23. What is VC (virtual circuit)?

If connection-oriented service is used, a path from the source router to the destination router must be established before any data packets can be sent. This connection is called a VC (virtual circuit):

24. What is Label Switching?

Avoiding conflicts of this kind is why routers need the ability to replace connection identifiers in outgoing packets. In some contexts, this is called label switching.

25. Define MPLS.

An example of a connection-oriented network service is MPLS (MultiProtocol Label Switching). It is used within ISP networks in the Internet, with IP packets wrapped in an MPLS header having a 20-bit connection identifier or label. MPLS is often hidden from customers, with the ISP establishing long-term connections for large amounts of traffic, but it is increasingly being used to help when quality of service is important but also with other ISP traffic management tasks.

26. What is mean by Ethernet?

Ethernet is a networking technology developed in 1970 which is governed by the IEEE 802.3 specifications. Ethernet is a Technology for connecting Local Area Networks.

27. Write the advantages of Ethernet.

1. Inexpensive 2. Easy to install 3.Supports various writing technologies.

28. What are the types of cabling?

Ethernet uses four types of cabling

- 10Base5 Thick coax
- 10Base2 Thin coax
- 10Base-T Twisted pair
- 10Base-F Fiber optics

29. What are the types of Ethernet?

There are several types of Ethernet networks, such as Fast Ethernet, Gigabit Ethernet, and Switched Ethernet.

30. Define Gigabit Ethernet?

Gigabit Ethernet is a version of the Ethernet technology broadly used in local area networks (LANs) for transmitting Ethernet frames at 1 Gbps. It is used as a backbone in many networks, particularly those of large organizations. Gigabit Ethernet is an extension to the preceding 10 Mbps and 100 Mbps 802.3 Ethernet standards. It supports 1,000 Mbps bandwidth while maintaining full compatibility with the installed base of around 100 million Ethernet nodes.

31. What is meant by exponential back-off?

It is a retransmission strategy that doubles the timeout value each time, when a packet is retransmitted. Once an adaptor has detected a collision and stopped its transmission, it waits a certain amount of time and tries again. Each time it tries to transmit but if it fails again, then the adaptor doubles the amount of time. This strategy of doubling the delay interval between each retransmission attempt is a general technique known as exponential back-off.

32. What is Manchester encoding?

Manchester encoding is an algorithm used in computer networking to digitally encode data bits. With Manchester encoding, data bits are represented in a series of different stages, which occur in a logical sequence. A negative-to-positive transition represents bit 1 and a positive-to-negative transition represents binary 0.

33. What is fast Ethernet?

Fast Ethernet is one of the versions of the Ethernet standard that enables the transmission of data over 100 megabits per second on local area networks (LAN). It was the fastest network connection of its time. Fast Ethernet is also known as 100 Base X or 100 Mbps Ethernet.

34. What is Adhoc Network?

An ad hoc network is a network that is composed of individual devices communicating with each other directly. The term implies spontaneous or impromptu construction because these networks often bypass the gatekeeping hardware or central access point such as a router. Many ad hoc networks are local area networks where

computers or other devices are enabled to send data directly to one another rather than going through a centralized access point.

35. What is the use of repeater?

A network device used to regenerate or replicate a signal. Repeaters are used in transmission systems to regenerate analog or digital signals distorted by transmission loss. Analog repeaters frequently can only amplify the signal while digital repeaters can reconstruct a signal to near its original quality. In a data network, a repeater can relay messages between sub networks that use different protocols or cable types. Hubs can operate as repeaters by relaying messages to all connected computers.

36. What is IEEE 802.11?

802.11 refers to a family of specifications developed by the IEEE for Wireless LAN (WLAN) technology. 802.11 specifies an over-the-air interface between a wireless client and a base station or between two wireless clients.

37. List the type of architecture used in IEEE 802.11. The type of architecture used in IEEE 802.11

- Infrastructure based
- Ad-hoc based

38. List out the applications of WLAN.

- Transfer of medical images
- Remote access to patient records
- Remote monitoring of patients
- Remote diagnosis of patients at home or in an ambulance
- In telemedicine
- Surveillance
- Internet supporting database.

39. What are the functions of MAC layer in IEEE 802.11?

The functions of MAC layer are

- Media Access Control
- Reliable delivery of data units

- Management functions
- Authentication encryption

40. Why are ad hoc networks needed?

Ad hoc networking is often needed where an infrastructure network cannot be deployed and managed. The presence of dynamic and adaptive routing protocols enables quick formation of ad hoc networks and is suitable for emergency situations like natural disasters, spontaneous meetings or military conflicts.

41. Define the Basic Service Set(BSS).

A basic service set is a group of stations communicating at physical layer level.

42. What are the categories of BSS?

- Infrastructure BSS – Here, the devices communicate with other devices through access points.
- Independent BSS – Here, the devices communicate in peer-to-peer basis in an ad hoc manner.

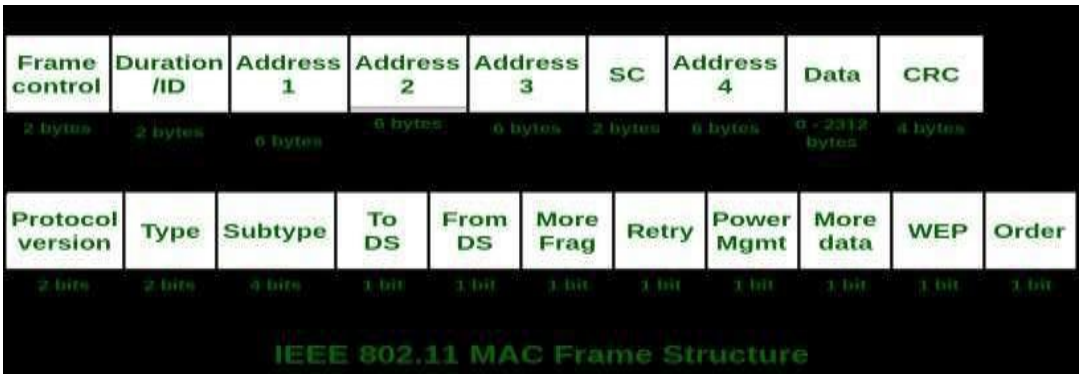
43. What is the Wireless Access Point(WAP)?

Wireless Access Points are generally wireless routers that form the base stations or access.

44. What are the services provided by IEEE 802.11?

- Association service is used by mobile stations to connect themselves to APs.
- Reassociation lets a station change its preferred AP. This facility is useful for mobile stations moving from one AP to another AP in the same extended 802.11 LAN.

45. Draw the MAC layer frame format of IEEE 802.11. The MAC layer frame format of IEEE 802.11



Explanatory Questions

1. Explain about various framing methods followed in data link layer (5 marks).
2. Discuss about error control and flow control (5 marks).
3. Explain Gigabit Ethernet (5 marks).
4. Explain Switched Ethernet (5 marks).
5. Explain Fast Ethernet (5 marks).
6. Write short notes on Pure and slotted ALOHA (5 marks).
7. Write short notes on persistent and non persistent CSMA protocols (5 marks).
8. Explain CSMA with collision detection protocol (5 marks).
9. Write short notes on (1) A bit map protocol (2) Binary countdown (5 marks)
10. Explain the MAC mechanism of IEEE 802.11 WLAN (5 marks).
11. Explain the 802.11 Mac Frame Structure (5 marks).
12. Explain the services defined by the 802.11 Standard (5 marks).
13. Explain the type of architecture used in IEEE 802.11 (5 marks).
14. Explain the 802.11 Physical layer (5 marks).
15. Discuss about data link layer design issues. (10 marks)
16. Write about channel allocation problem in detail. (10 marks)
17. Explain the Ethernet MAC Sub layer protocol. (10 marks)
18. Explain different multiple access protocol. (10 marks)

19. Discuss about various ethernet mechanism used in computer network. (10 marks)

20. Explain the Wireless LAN – 802.11 Architecture. (10 marks)

Objective Questions and Answers

1. Which among the following represents the objectives/requirements of Data Link Layer?

    a. Frame Synchronization

    b. Error & Flow Control

    c. Both a & b

    d. None of the above

    Answer: c. Both a & b

2. What are the frames issued by the secondary station of HDLC, known as?

    a. Link

    b. Command

    c. Response

    d. None of the above

    Answer: c. Response

3. Which one of the following tasks is not done by data link layer?

    a. framing

    b. error control

    c. flow control

    d. channel coding

    Answer: d. channel coding

4. Two main functions of data link layer are

    a. hardware link control and media access control

    b. data link control and protocol access control

    c. data link control and media access control

    d. both a and c

    Answer: c. data link control and media access control

5. Which of the following devices is a PC component that connects the computer to

the network?

a. Bridge

b. NIC (Network Interface Card)

c. DNS Server

d. Gateway

Answer: b. NIC(Network Interface Card)

6. Switch is a Device of_____Layer of OSI Model.

a. Network Layer

b. Data Link Layer

c. Application Layer

d. Session Layer

Answer: b. Data Link Layer

7. When 2 or more bits in a data unit has been changed during the transmission, the error is called

a. random error

b. burst error

c. inverted error

d. none of the mentioned

Answer: b. burst error

8. How the error detection is achieved at data link layer?

a. Hamming codes

b. Bit stuffing

c. Detection manager

d. None of the above

Answer: b. Bit Stuffing

9. Bridge works in which layer of the OSI model?

a. Application layer

b. Transport layer

c. Network layer

d. Data link layer

Answer: d .Data link layer.

10. HDLC is an acronym for_____.

    a. High-duplex line communication

    b. High-level data link control

    c. Half-duplex digital link combination

    d. Host double-level circuit

    Answer: b. High-Level data link control

11. Data link control deals with the design and procedures for_____communication.

    a. node-to-node

    b. host-to-host

    c. process-to-process

    d. none of the above

    Answer: a. node-to-node

12. In_____protocols, we use_____.

    a. character-oriented; byte stuffing

    b. character-oriented; bit stuffing

    c. bit-oriented; character stuffing

    d. none of the above

    Answer: a . character-oriented; byte stuffing.

13. Byte stuffing means adding a special byte to the data section of the frame when there is a character with the same pattern as the__.

    a. Header

    b. trailer

    c. flag

    d. none of the above

    Answer: c. flag.

14. In fixed channel assignment strategy, each cell is allocated a predetermined set of _____

    a. Voice channels

    b. Control channels

    c. Frequency

    d. base stations

Answer : a

15. What happen to a call in fixed channel strategy, if all the channels in a cell are occupied?

    a. Queued
    b. Cross talk
    c. Blocked
    d. Delayed

Answer : c

16. What is a borrowing strategy in fixed channel assignments?

    a. Borrowing channels from neighbouring cell
    b. Borrowing channels from neighbouring cluster
    c. Borrowing channels from same cell
    d. Borrowing channels from other base station in same cell

Answer : a

17. In dynamic channel assignment strategy, voice channels are---------- to different cells.

    a. Allocated Permanently
    b. Not Allocated Permanently
    c. Allocated time based
    d. Allocated frequency based

Answer : b

18. In dynamic channel assignment strategy, base station requests channel from _____

    a. MSC
    b. Neighbouring cell
    c. Neighbouring cluster
    d. Neighbouring base station

Answer : a

19. Lower sub layer of the data link layer is responsible for

    a. multiple access
    b. point to point access
    c. error detection
    d. flow control

Answer : a

20. In_____, each station sends a frame whenever it has a frame to send.

    a. Pure ALOHA
    b. Slotted ALOHA
    c. Both a and b
    d. Neither a nor b

Answer : a

21. In pure ALOHA, the vulnerable time is_____the frame transmission time.

    a. The same as
    b. Two times
    c. Three times
    d. None of the above

Answer : b

22. The maximum throughput for the pure

    ALOHA is a. 12.2

b. 18.4

c. 36.8

d. 32.2

Answer : b

23. In_____, each station is forced to send only at beginning of the time slot

    a. Pure ALOHA
    b. Slotted ALOHA
    c. Both a and b
    d. Neither a nor b

Answer : b

24. In slotted ALOHA, the vulnerable time is_____the frame transmission time.

    a. The same as
    b. Two times
    c. Three times
    d. None of the above

Answer : a

25. The maximum throughput for the pure ALOHA is a. 12.2
    b. 18.4
    c. 36.8
    d. 32.2

Answer : c

26. In Carrier Sense Multiple Access (CSMA), if station senses medium before trying to use it then chance of collision can be
    a. Increased
    b. Reduced
    c. Highlighted
    d. Both

B & **C Answer : b**

27. Code Division Multiple Access (CDMA) differs from Time Division Multiple Access (TDMA) because there is no
    a. bandwidth
    b. link
    c. carrier
    d. timesharing

Answer : d

28. In Carrier Sense Multiple Access (CSMA), possibility of collision still exist because of
    a. Propagation delay
    b. sender-receiver delay
    c. Sense delay
    d. Transmit delay

Answer : a

29. Protocol that is used to transmit data without any schedule time is
    a. random access
    b. controlled access
    c. channelization
    d. none of the above

Answer : a

30. Carrier Sense Multiple Access (CSMA) is based on medium called

    a. Listen before talk
    b. Listen before sending
    c. Sense before transmit
    d. Sense before Collision

Answer : c

31. In_____, a station monitors the medium after it sends a frame to see if the transmission was successful. If so, the station is finished. If, however, there is a collision, the frame is sent again.

    a. CSMA/CA
    b. CSMA/CD
    c. MA
    d. None of the above

Answer : b

32. To avoid collision on wireless networks,_____was invented.

    a. CSMA/CA
    b. CSMA/CD
    c. MA
    d. None of the above

Answer : a

33. IEEE 802.11 defines basic service set as building block of a wireless

    a) LAN

    b) WAN protocol

    c) MAN

    d) All of the above

Answer: a

34. What is the access point (AP) in wireless LAN?

    a) device that allows wireless devices to connect to a wired network
    b) wireless devices itself

c) both device that allows wireless devices to connect to a wired network and wireless devices itself

d) none of the mentioned

Answer: a

a) frames
b) fields
c) signals

35. IEEE 802.11 have three categories of

sequences

Answer: a

36. In wireless ad-hoc network

a) access point is not required

b) access point is must

c) nodes are not required

Answer: a

d) none of the mentioned

37. Which multiple access technique is used by IEEE 802.11 standard for wireless LAN?

a) CDMA

b) CSMA/CA

c) ALOHA

Answer: b

d) None of the mentioned

38. In wireless distribution system

a) multiple access point are inter-connected with each other

b) there is no access point

c) only one access point exists

Answer: a

d) none of the mentioned

39. A wireless network interface controller can work in

a) infrastructure mode

b) ad-hoc mode

c) both infrastructure mode and ad-hoc mode

Answer: c

d) none of the mentioned

40. In wireless network an extended service set is a set of

a) all connected basic service sets

b) all stations

c) all access points

Answer: a

d) none of the mentioned

41. Mostly_____is used in wireless LAN.

a) time division multiplexing

b) orthogonal frequency division multiplexing

c) space division multiplexing

Answer: b

d) none of the mentioned

42. Which one of the following event is not possible in wireless LAN

a) collision detection

b) acknowledgement of data frames

c) multi-mode data transmission

d) none of the mentioned

Answer: a

43. The service used by mobile stations to connect themselves to APs is.

a) collision avoidance

b) association

c) collision detection

d) reassociation

Answer: b

44. The service used by mobile stations to change its preferred AP is.

a) collision avoidance

b) collision detection

c) association

d) reassociation

Answer: d

45. DCF stands for

a) Direct Control Function

b) Distributed Control Function

c) Direct Cooperate Function

d) Distributed Coordination Function

Answer: d

46. PCF stands for

a) Point Coordination Function

b) Point Control Function

c) Process Control Function

d) Process Coordination Function

Answer: a

47. Current version in frame control field is

a) 0

b) 1

c) 2

d) 3

Answer: a