KarpagamAcademy of Higher Education
(Established Under Section 3 of UGC Act 1956)
Eachanari Post, Coimbatore – 641 021. INDIA
Phone : 0422-2611146, 2611082 Fax No : 0422 -2611043

17CAU303 **COMPUTER NETWORKS** **4H – 4C**

Instruction Hours / week: L: 4 T: 0 P: 0 **Marks:** Int : **40** Ext : **60** Total: **100**

Scope

The course include basics of switched communication networks, TCP/IP networking, network programming, packet switch architecture, rate and congestion control, Quality-of-Service networks, wireless communications.

Objectives

Various transmission media, their comparative study, fiber optics and wireless media

Categories and topologies of networks (LAN and WAN) Layered architecture (OSI and TCP/IP) and protocol suites.

Channel error detection and correction, MAC protocols, Ethernet and WLAN.

Details of IP operations in the INTERNET and associated routing principles

Unit- I

Introduction to Computer Networks : Network definition; network topologies; network classifications; network protocol; layered network architecture; overview of OSI reference model; overview of TCP/IP protocol suite. **Data Communication Fundamentals and Techniques**: Analog and digital signal; data-ratelimits; digital to digital line encoding schemes; pulse code modulation; parallel and serial transmission;

Unit-II

Digital to analog modulation-; multiplexing techniques- FDM, TDM; transmission media.

Networks Switching Techniques and Access mechanisms: Circuit switching; packetswitching - connectionless datagram switching, connection-oriented virtual circuit switching; dial-up modems; digital subscriber line; cable TV for data transfer.

Unit-III

Data Link Layer Functions and Protocol: Error detection and error correction techniques;
data-link control- framing and flow control; error recovery protocols- stop and wait ARQ, go-back-n ARQ; Point to Point Protocol on Internet.

Semester – III

17CAU303 COMPUTER NETWORKS 4H – 4C

Unit-IV

Multiple Access Protocol and Networks: CSMA/CD protocols; Ethernet LANS; connecting LAN and back-bone networks- repeaters, hubs, switches, bridges, router and gateways;

Networks Layer Functions and Protocols: Routing; routing algorithms; network layer protocol of Internet- IP protocol, Internet control protocols.

Unit-V

Transport Layer Functions and Protocols: Transport services- error and flow control, Connection establishment and release- three way handshake;

Overview of Application layer protocol: Overview of DNS protocol; overview of WWW &HTTP protocol.

Suggested readings

1. Forouzan B. A., (2007). *Data Communications and Networking,* (4th ed.), THM.
2. Tanenbaum, A. S. , (2002). Computer Networks**,** (4th ed.), PHI.

Websites

1. en.wikipedia.org/wiki/Internet_protocol_suite
2. http://docwiki.cisco.com/wiki/Introduction_to_WAN_Technologies
3. www.yale.edu/pclt/COMM/**TCPIP**.HTM
4. www.w3schools.com/**tcpip**/default.asp
5. https://www.cse.iitb.ac.in/

COURSE NAME: COMPUTER NETWORKS **COURSE CODE: 17CAU303**

LECTURE PLAN

UNIT I

S. No	Lecturer Duration(Hrs)	Topics to be Covered	Support Materials
1	1	Introduction to Computer Networks: Network Definition, Network Topologies	T1: 7-16, W1
2	1	Network Classifications, Network Protocols	T1: 17-19, W1
3	1	Layered Network Architecture: Overview of OSI Reference Model	T1: 30-41
4	1	Overview of TCP/IP Protocol Suite	T1: 41-45
5	1	Data Communication Fundamentals and Techniques: Analog and Digital Signal, Data-rate Limits	T1: 57-59 T1: 85-87
6	1	Digital- Digital Line Encoding Schemes	T1: 106-115
7	1	Pulse Code Modulation	T1: 121-129
8	1	Parallel and Serial Transmission	T1: 131-135
9	1	Recapitulation and Discussion of important questions	
Total No .of Hours Planed For Unit I : 9 Hours			

Textbooks:

T1: Forouzan B. A., (2007). Data Communications and Networking, (4th ed.), THM.

Websites:

W1: http://docwiki.cisco.com/wiki/Introduction_to_WAN_Technologies

LECTURE PLAN

UNIT II

S. No	Lecturer Duration(Hrs)	Topics to be covered	Support Materials
1.	1	Digital to Analog Modulation	T1: 141-148
2.	1	Multiplexing Techniques - FDM - TDM	T1: 162-180
3.	1	Transmission Media	T1: 191-208
4.	1	Networks Switching Techniques and Access Mechanisms: Circuit Switching, Packet Switching	T1: 213-217, W2
5.	1	Connection less Datagram Switching	T1: 218-221
6.	1	Connection-Oriented Virtual Circuit Switching	T1: 221-227
7.	1	Dial-Up Modems, Digital Subscriber Line	T1: 248-257, W2
8.	1	Cable TV for Data Transfer	T1: 257-261
9.	1	Recapitulation and Discussion of important questions	
Total No .of Hours Planed For Unit II : 9 Hours			

Textbooks:

T1: Forouzan B. A., (2007). Data Communications and Networking, (4th ed.), THM.

Websites:

W2: https://www.cse.iitb.ac.in/

LECTURE PLAN

UNIT III

S. No	Lecturer Duration(Hrs)	Topics to be covered	Support Materials
1.	1	Data Link Layer Functions and Protocols: Error Correction & Detection Techniques	T1: 267-270, W3
2.	1	Introduction Block Coding	T1: 271-277
3.	1	Linear Block Codes	T1: 277-284
4.	1	Cyclic Codes, Checksum	T1: 284-300
6.	1	Data Link Control: Framing and Flow Control	T1: 307-311, W3
8.	1	Error Recovery Protocols - Stop and Wait ARQ	T1: 311 T1: 318-324
10.	1	Go-Back- N ARQ	T1: 324-330
11.	1	Point to Point Protocol on Internet	T1: 346-350
12.	1	Recapitulation and Discussion of important questions	
Total No .of Hours Planed For Unit III : 9 Hours			

Textbooks:

T1: Forouzan B. A., (2007). Data Communications and Networking, (4th ed.), THM.

Websites:

W3: www.geeksforgeeks.org/Computer-network-tutorials

LECTURE PLAN

UNIT IV

S. No	Lecturer Duration(Hrs)	Topics to be covered	Support Materials
1.	1	Multiple Access Protocol and Networks CSMA/CD Protocols	T1: 373-377
2.	1	Ethernet LANs	T1: 395-415
3.	1	Connecting LAN and back-bone networks: Repeaters, Hubs, Switches, Bridges	T1: 445-456
4.	1	Router and Gateways	T1: 451-456
5.	1	Network Layer Functions and Protocols: Routing, Routing Algorithms	T1: 350-360
6.	1	Network Layer Protocol of Internet IP Protocol	T1: 433-434,W4
7.	1	IPV4 Datagram Format	T1: 434-436,W4
8.	1	Internet Control Protocols	T1: 449-454, W4
9.	1	Recapitulation and Discussion of important questions	
Total No .of Hours Planed For Unit IV : 9 Hours			

Textbooks:

T1: Forouzan B. A., (2007). Data Communications and Networking, (4th ed.), THM.

T2: Tanenbaum, A. S. , (2002). Computer Networks**,** (4th ed.), PHI.

Websites:

W4: http://docwiki.cisco.com/wiki/Introduction_to_WAN_Technologies

LECTURER PLAN

UNIT V

S. No	Lecturer Duration(Hrs)	Topics to be covered	Support Materials
1.	1	Transport Layer Functions and protocols: Transport Services	T1: 715-723
2.	1	Error and Flow Control	T1: 728-735
3.	1	Connection Establishment and Release	T1: 723-725, W5
4.	1	Three Way Handshake	T1: 726-728, W5
5.	1	Overview of Application Layer Protocol	T2: 579-582
6.		Overview of DNS Protocol	T2: 583-586
7.	1	Overview of WWW	T2: 612-643
8.	1	HTTP Protocol	T2: 651-655
9.	1	Recapitulation and Discussion of important questions	
10.	1	Discussion on previous ESE question papers	
11.	1	Discussion on previous ESE question papers	
12.	1	Discussion on previous ESE question papers	
Total No .of Hours Planed For Unit V : 12 Hours			

Textbooks:

Textbooks:

T1: Forouzan B. A., (2007). Data Communications and Networking, (4th ed.), THM.

T2: Tanenbaum, A. S. , (2002). Computer Networks**,** (4th ed.), PHI.

Websites:

W5: https://www.cse.iitb.ac.in/

INTRODUCTION TO COMPUTER NETWORKS

Network Definition:

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

Network Topologies:

The arrangement of a network which comprises of nodes and connecting lines via sender and receiver is referred as network topology. The various network topologies are :

a) Mesh Topology:

In mesh topology, every device is connected to another device via particular channel.

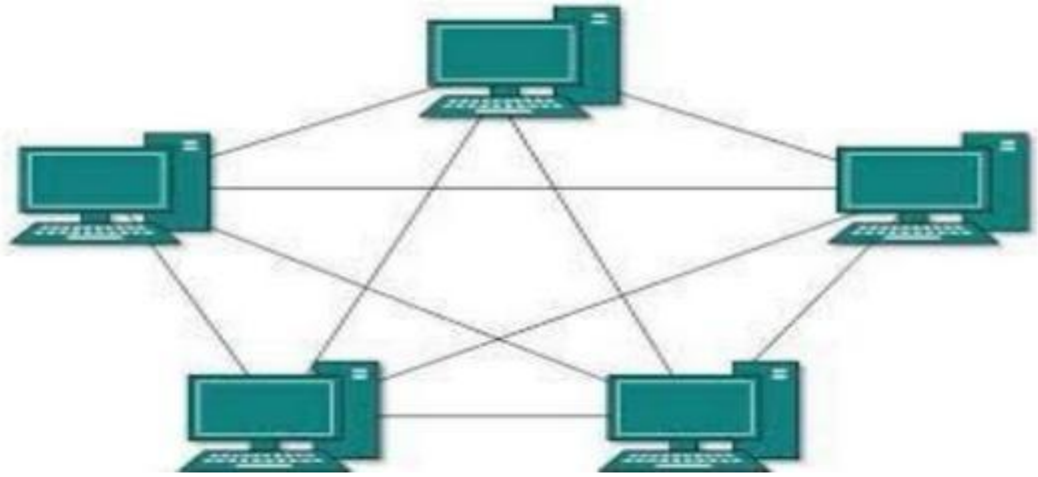


Figure 1 : Every device is connected with another via dedicated channels. These channels are known as links.

If suppose, N number of devices are connected with each other in mesh topology, then total number of ports that is required by each device is N-1. In the Figure 1, there are 5 devices connected to each other, hence total number of ports required is 4.

If suppose, N number of devices are connected with each other in mesh topology, then total number of dedicated links required to connect them is ${}^{N}C_{2}$ i.e. N(N-1)/2. In the Figure 1, there are 5 devices connected to each other, hence total number of links required is 5*4/2 = 10.

Advantages of this topology :

It is robust.

Fault is diagnosed easily. Data is reliable because data is transferred among the devices through dedicated channels or links.

Provides security and privacy.

Problems with this topology :

Installation and configuration is difficult.

Cost of cables are high as bulk wiring is required, hence suitable for less number of devices.

Cost of maintenance is high.

b) Star Topology:

In star topology, all the devices are connected to a single hub through a cable. This hub is the central node and all others nodes are connected to the central node. The hub can be passive in nature i.e. not intelligent hub such as broadcasting devices, at the same time the hub can be intelligent known as active hubs. Active hubs have repeaters in them.

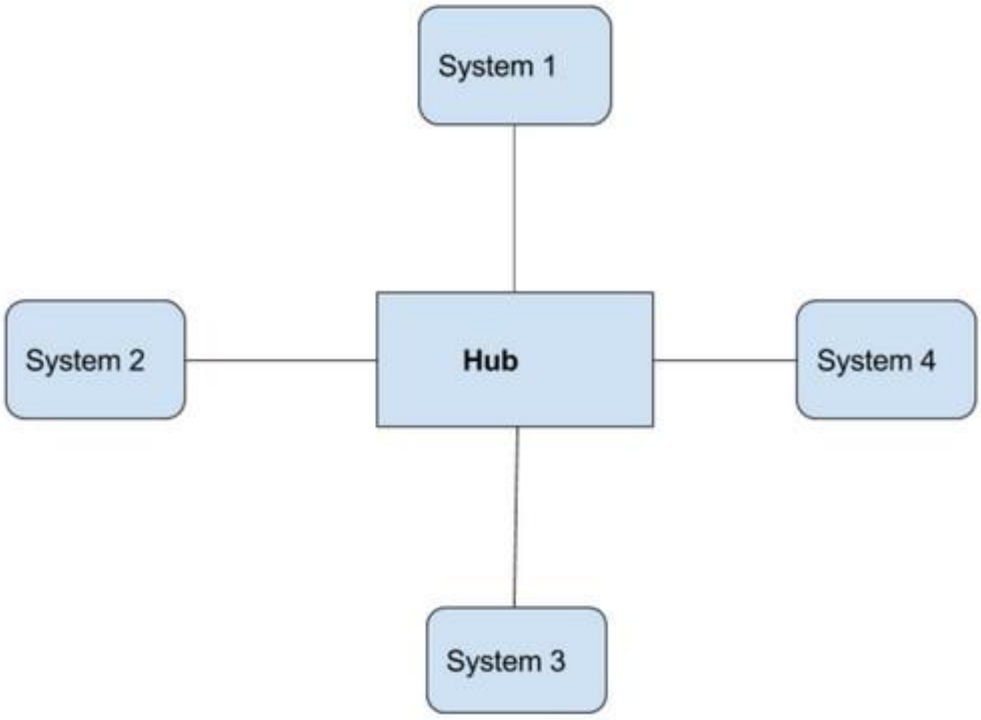


Figure 2 : A star topology having four systems connected to single point of connection i.e. hub.

Advantages of this topology:

If N devices are connected to each other in star topology, then the number of cables required to connect them is N. So, it is easy to set up.

Each device requires only 1 port i.e. to connect to the hub.

Problems with this topology:

If the concentrator (hub) on which the whole topology relies fails, the whole system will crash down.

Cost of installation is high.
Performance is based on the single concentrator i.e. hub.

c) Bus Topology :

Bus topology is a network type in which every computer and network device is connected to single cable. It transmits the data from one end to another in single direction. No bi-directional feature is in bus topology.

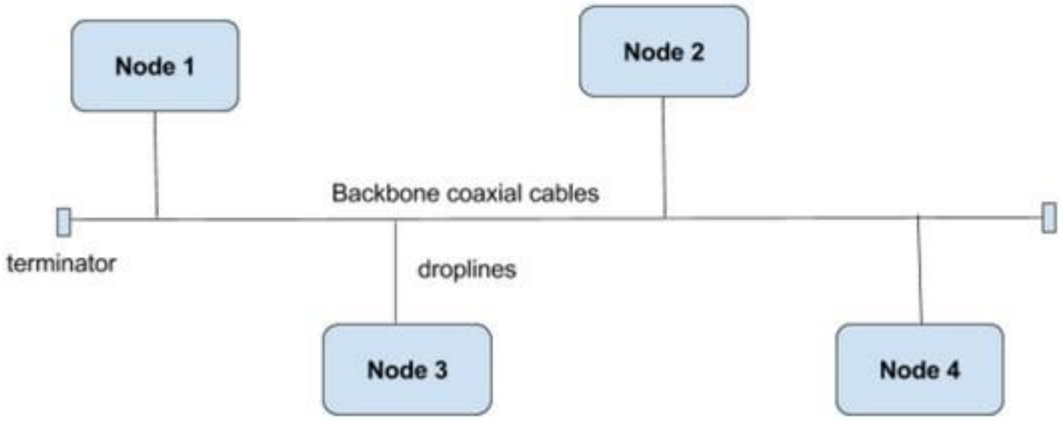


Figure 3 : A bus topology with shared backbone cable. The nodes are connected to the channel via drop lines.

Advantages of this topology :

If N devices are connected to each other in bus topology, then the number of cables required to connect them is 1 which is known as backbone cable and N drop lines are required.

Cost of the cable is less as compared to other topology, but it is used to built small networks.

Problems with this topology :

If the common cable fails, then the whole system will crash down.

If the network traffic is heavy, it increases collisions in the network. To avoid this, various protocols are used in MAC layer known as Pure Aloha, Slotted Aloha, CSMA/CD etc.

d) Ring Topology :

In this topology, it forms a ring connecting a devices with its exactly two neighbouring devices.

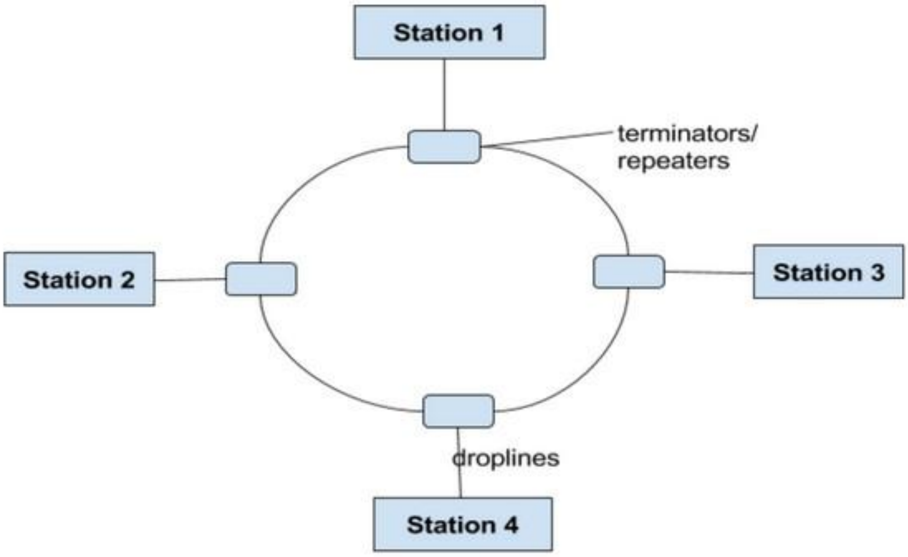


Figure 4 : A ring topology comprises of 4 stations connected with each forming a ring..

The following operations takes place in ring topology are :

1. One station is known as **monitor** station which takes all the responsibility to perform the operations.
2. To transmit the data, station has to hold the token. After the transmission is done, the token is to be released for other stations to use.
3. When no station is transmitting the data, then the token will circulate in the ring.
4. There are two types of token release techniques : **Early token release** releases the token just after the transmitting the data and **Delay token release** releases the token after the acknowledgement is received from the receiver.

Advantages of this topology :

The possibility of collision is minimum in this type of topology.

Cheap to install and expand.

Problems with this topology :

Troubleshooting is difficult in this topology.

Addition of stations in between or removal of stations can disturb the whole topology.

e) Hybrid Topology:

This topology is a collection of two or more topologies which are described above. This is a scalable topology which can be expanded easily. It is reliable one but at the same it is a costly topology.

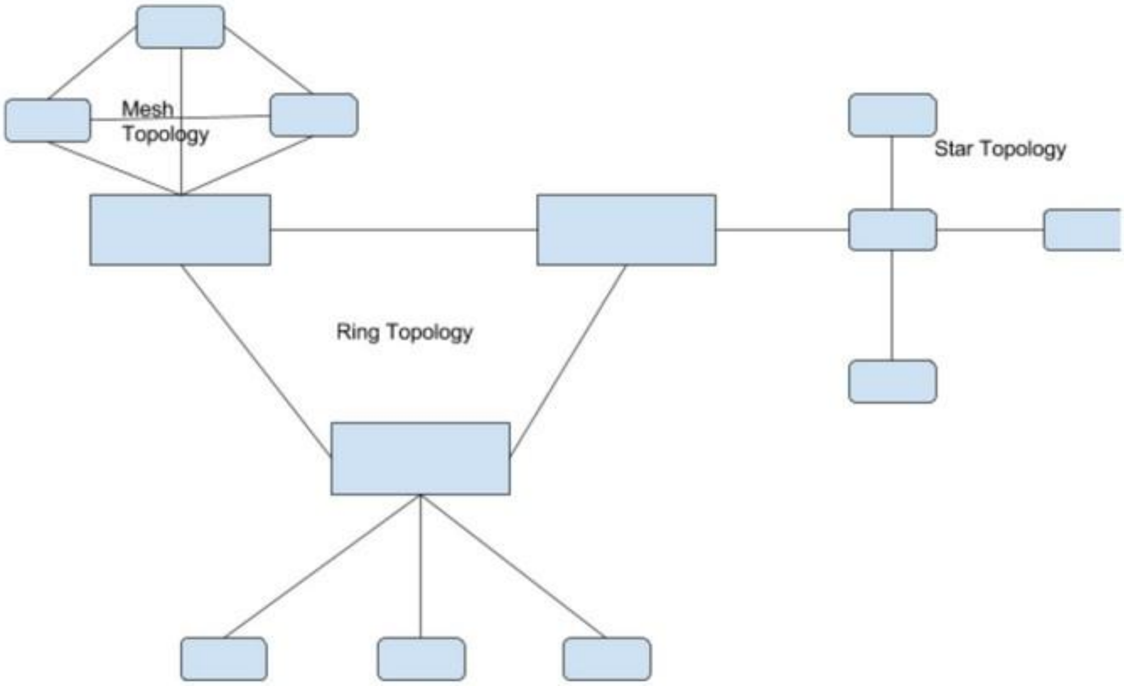


Figure 5 : A hybrid topology

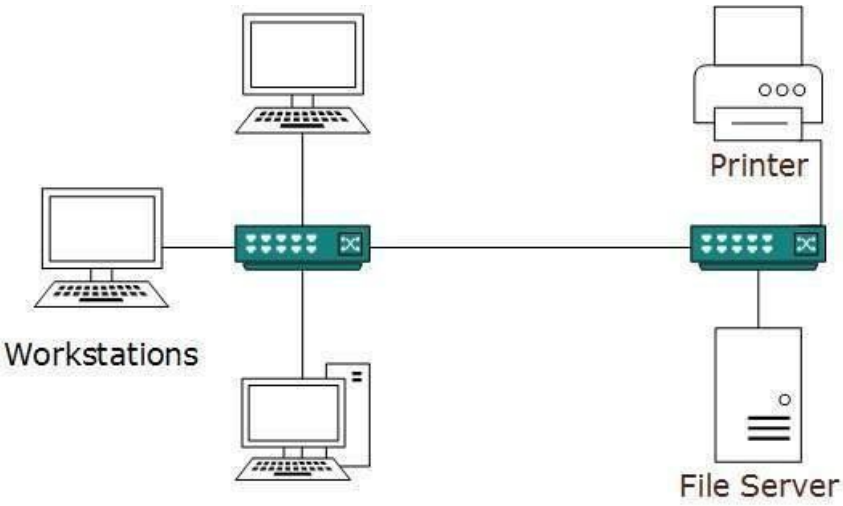
Figure 5 : A hybrid topology which is a combination of ring and star topology.

Network Classifications:

LocalArea Network:

A computer network spanned inside a building and operated under single administrative system is generally termed as Local Area Network (LAN). Usually, LAN covers an organization' offices, schools, colleges or universities. Number of systems connected in LAN may vary from as least as two to as much as 16 million.

LAN provides a useful way of sharing the resources between end users. The resources such as printers, file servers, scanners, and internet are easily sharable among computers.



LANs are composed of inexpensive networking and routing equipment. It may contains local servers serving file storage and other locally shared applications. It mostly operates on private IP addresses and does not involve heavy routing. LAN works under its own local domain and controlled centrally.

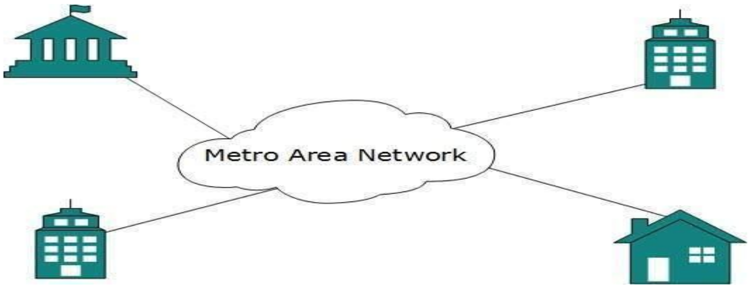
LAN uses either Ethernet or Token-ring technology. Ethernet is most widely employed LAN technology and uses Star topology, while Token-ring is rarely seen.

LAN can be wired, wireless, or in both forms at once.

MetropolitanArea Network:

The Metropolitan Area Network (MAN) generally expands throughout a city such as cable TV network. It can be in the form of Ethernet, Token-ring, ATM, or Fiber Distributed Data Interface (FDDI).

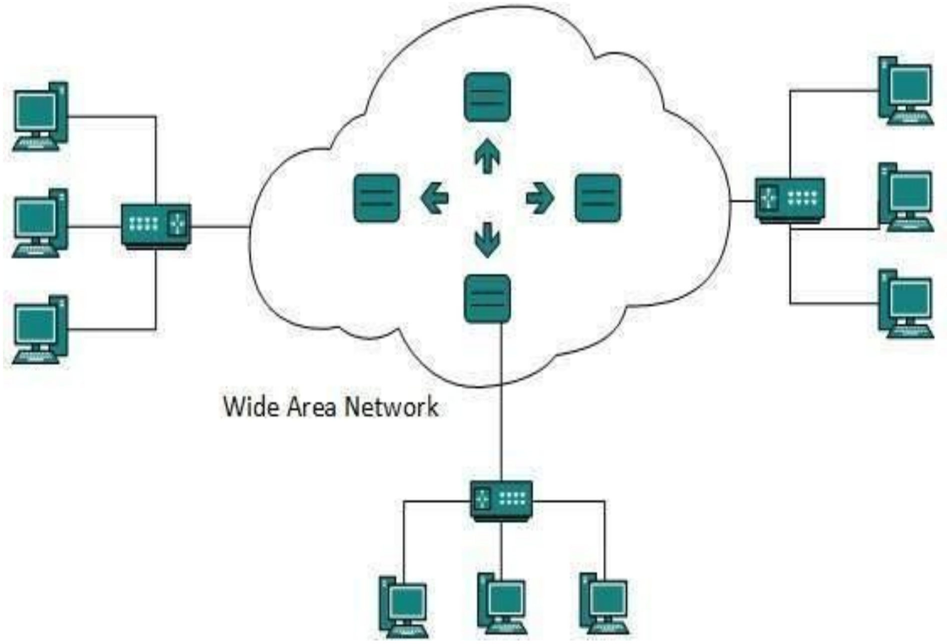
Metro Ethernet is a service which is provided by ISPs. This service enables its users to expand their Local Area Networks. For example, MAN can help an organization to connect all of its offices in a city.



Backbone of MAN is high-capacity and high-speed fiber optics. MAN works in between Local Area Network and Wide Area Network. MAN provides uplink for LANs to WANs or internet.

Wide Area Network:

As the name suggests, the Wide Area Network (WAN) covers a wide area which may span across provinces and even a whole country. Generally, telecommunication networks are Wide Area Network. These networks provide connectivity to MANs and LANs. Since they are equipped with very high speed backbone, WANs use very expensive network equipment.



WAN may use advanced technologies such as Asynchronous Transfer Mode (ATM), Frame Relay, and Synchronous Optical Network (SONET). WAN may be managed by multiple administrations.

Internetwork:

A network of networks is called an internetwork, or simply the internet. It is the largest network in existence on this planet. The internet hugely connects all WANs and it can have connection to LANs and Home networks. Internet uses TCP/IP protocol suite and uses IP as its addressing protocol. Present day, Internet is widely implemented using IPv4. Because of shortage of address spaces, it is gradually migrating from IPv4 to IPv6.

Internet enables its users to share and access enormous amount of information worldwide. It uses WWW, FTP, email services, audio and video streaming etc. At huge level, internet works on Client-Server model.

Internet uses very high speed backbone of fiber optics. To inter-connect various continents, fibers are laid under sea known to us as submarine communication cable.

Internet is widely deployed on World Wide Web services using HTML linked pages and is accessible by client software known as Web Browsers. When a user requests a page using some web browser located on some Web Server anywhere in the world, the Web Server responds with the proper HTML page. The communication delay is very low.

Internet is serving many proposes and is involved in many aspects of life. Some of them are:

Web sites

E-mail

Instant Messaging

Blogging
Social Media
Marketing
Networking
Resource Sharing
Audio and Video Streaming

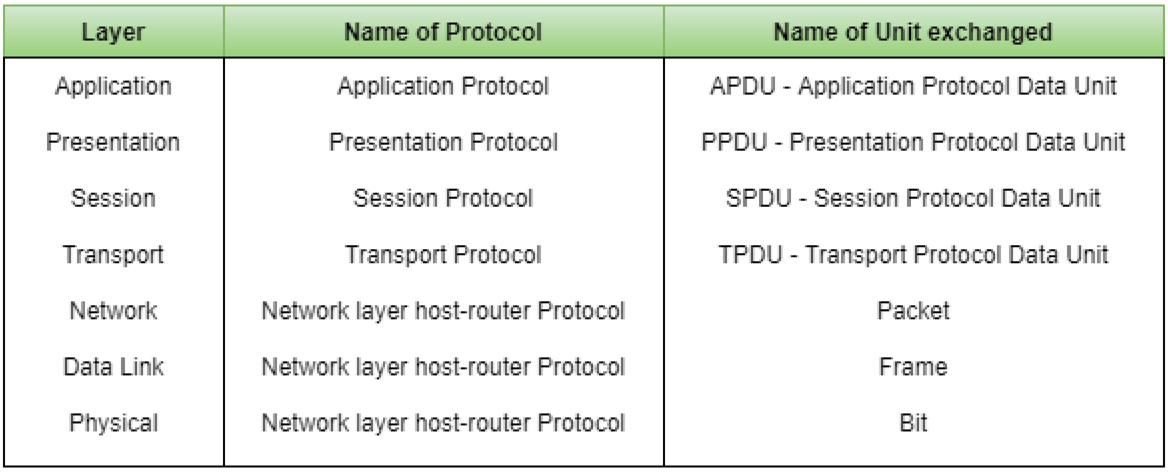
Protocols

- A protocol is a set of rules that governs data communications
- It defines what is communicated, how it is communicated and when it is communicated
- Key elements of a protocol:
    - —**Syntax**
        - Structure or format of data, meaning the order in which they are presented
    - —**Semantics**
        - Refer to the meaning of each section of bits, how a particular pattern is interpreted and what action to be taken
    - —**Timing**
        - Refers to when data should be sent and how fast can they be sent

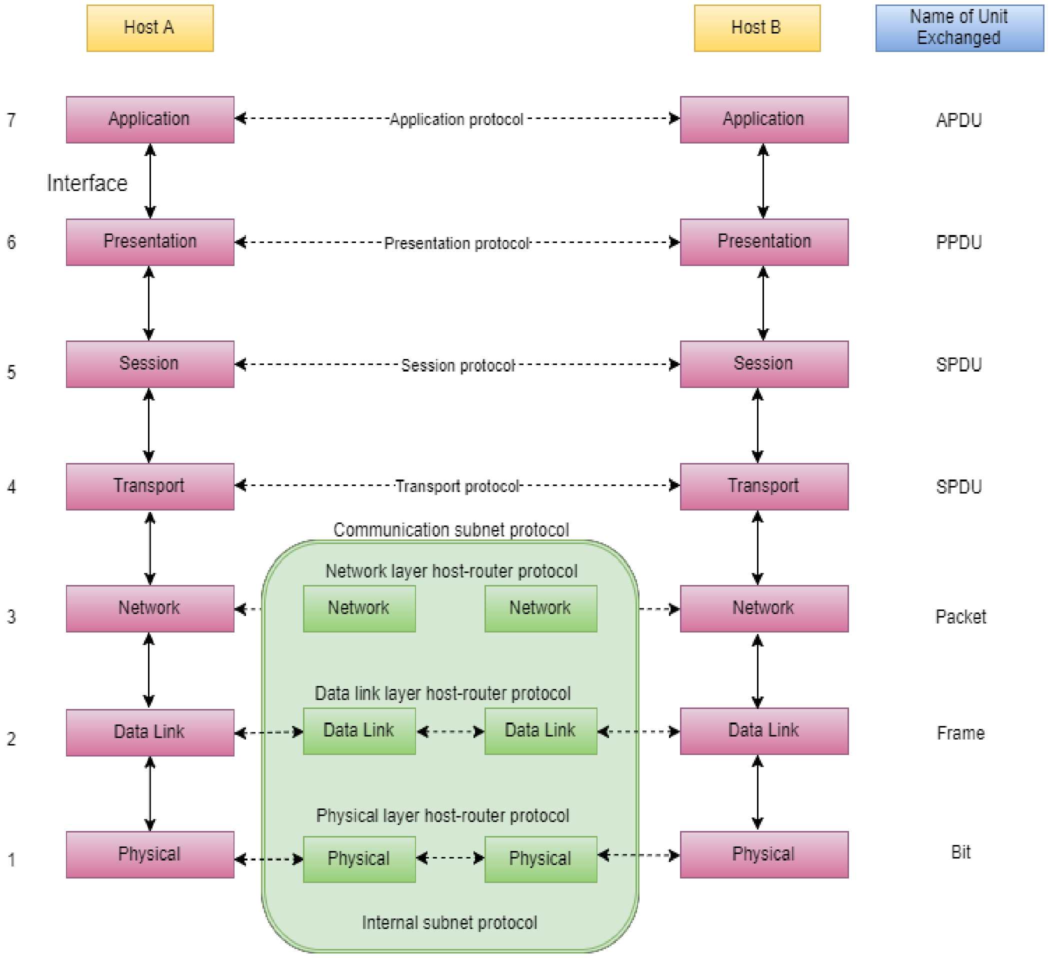
Overview of OSI Reference Model

OSI stands for **Open Systems Interconnection**. It has been developed by ISO – **International Organization of Standardization**‘, in the year 1974. The ISO-OSI model is a seven layer architecture. All these 7 layers work collaboratively to transmit the data from one person to another across the globe.

The ISO-OSI model is seven layer architecture. It defines seven layers or levels in a complete communication system.



Layer	Name of Protocol	Name of Unit exchanged
Application	Application Protocol	APDU - Application Protocol Data Unit
Presentation	Presentation Protocol	PPDU - Presentation Protocol Data Unit
Session	Session Protocol	SPDU - Session Protocol Data Unit
Transport	Transport Protocol	TPDU - Transport Protocol Data Unit
Network	Network layer host-router Protocol	Packet
Data Link	Network layer host-router Protocol	Frame
Physical	Network layer host-router Protocol	Bit



The Physical Layer: (Layer 1)

1. It is the lowest layer of the OSI Model.
2. It activates, maintains and deactivates the physical connection.
3. It is responsible for transmission and reception of the unstructured raw data over network.
4. Voltages and data rates needed for transmission is defined in the physical layer.
5. It converts the digital/analog bits into electrical signal or optical signals.
6. Data encoding is also done in this layer.
7. The functions of this layer are Physical characteristics of interfaces and media, Representation of bits, Data rate, Synchronization of bits, Line configuration, Physical topology and Transmission mode.

Data Link Layer: (Layer 2)

1. Data link layer synchronizes the information which is to be transmitted over the physical layer.
2. The main function of this layer is to make sure data transfer is error free from one node to another, over the physical layer.
3. Transmitting and receiving data frames sequentially is managed by this layer.

4. This layer sends and expects acknowledgements for frames received and sent respectively. Resending of non-acknowledgement received frames is also handled by this layer.
5. This layer establishes a logical layer between two nodes and also manages the Frame traffic control over the network. It signals the transmitting node to stop, when the frame buffers are full.
6. The functions of this layer are Framing, Physical addressing, Flow control, Error control and Access control

The Network Layer: (Layer 3)

1. It routes the signal through different channels from one node to other.
2. It acts as a network controller. It manages the Subnet traffic.
3. It decides by which route data should take.
4. It divides the outgoing messages into packets and assembles the incoming packets into messages for higher levels.
5. The functions of this layer are Logical addressing and Routing

The Transport Layer: (Layer 4)

1. It decides if data transmission should be on parallel path or single path.
2. Functions such as Multiplexing, Segmenting or Splitting on the data are done by this layer
3. It receives messages from the Session layer above it, converts the message into smaller units and passes it on to the Network layer.
4. Transport layer can be very complex, depending upon the network requirements.
5. Transport layer breaks the message (data) into small units so that they are handled more efficiently by the network layer.
6. The functions of the Transport layer are Service-point (port) addressing, Segmentation and reassembly, Connection control, Flow control and Error control

The Session Layer: (Layer 5)

1. Session layer manages and synchronize the conversation between two different applications.
2. Transfer of data from source to destination session layer streams of data are marked and are resynchronized properly, so that the ends of the messages are not cut prematurely and data loss is avoided.
3. The functions of this layer are Session establishment, maintenance and termination, Synchronization and Dialog Controller

The Presentation Layer: (Layer 6)

1. Presentation layer takes care that the data is sent in such a way that the receiver will understand the information (data) and will be able to use the data.
2. While receiving the data, presentation layer transforms the data to be ready for the application layer.
3. Languages (syntax) can be different of the two communicating systems. Under this condition presentation layer plays a role of translator.
4. The functions of the Presentation layer are Translation, Encryption/ Decryption and Compression

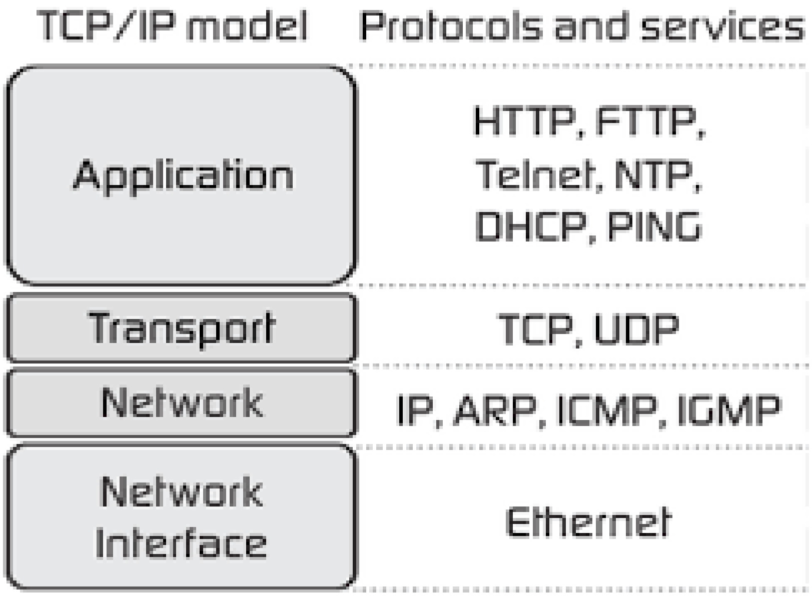
Application Layer: (Layer 7)

1. It is the topmost layer.
2. This layer mainly holds application programs to act upon the received and to be sent data.
3. The functions of this layer are Network Virtual Terminal, FTAM-File transfer access and management, Mail Services and Directory Services

Overview of TCP/IP Suite:

The **TCP/IP model** is a concise version of the OSI model. It contains four layers, unlike seven layers in the OSI model.

:



TCP/IP model	Protocols and services
Application	HTTP, FTTP, Telnet, NTP, DHCP, PING
Transport	TCP, UDP
Network	IP, ARP, ICMP, IGMP
Network Interface	Ethernet

Network Interface Layer:

1. It is also called as Host-to-network layer.
2. Lowest layer of the all.
3. Protocol is used to connect to the host, so that the packets can be sent over it.
4. Varies from host to host and network to network.

Internet layer:

1. Selection of a packet switching network which is based on a connectionless internetwork layer is called a internet layer.
2. It is the layer which holds the whole architecture together.
3. It helps the packet to travel independently to the destination.
4. Order in which packets are received is different from the way they are sent.
5. IP (Internet Protocol) is used in this layer.
6. The main protocols residing at this layer are :

   IP – stands for Internet Protocol and it is responsible for delivering packets from the source host to the destination host by looking at the IP addresses in the packet headers.

   ICMP – stands for Internet Control Message Protocol. It is encapsulated within IP datagrams and is responsible for providing hosts with information about network problems.

   ARP – stands for Address Resolution Protocol. It's job is to find the hardware address of a host from a known IP address. ARP has several types: Reverse ARP, Proxy ARP, Gratituous ARP and Inverse ARP.

Transport Layer:

1. It decides if data transmission should be on parallel path or single path.
2. Functions such as multiplexing, segmenting or splitting on the data is done by transport layer.
3. The applications can read and write to the transport layer.
4. Transport layer adds header information to the data.
5. Transport layer breaks the message (data) into small units so that they are handled more efficiently by the network layer.
6. Transport layer also arrange the packets to be sent, in sequence.
7. The two main protocols present in this layer are:

   Transmission Control Protocol (TCP) – It is known to provide reliable and error-free communication between end systems. It performs sequencing and segmentation of data. It also has acknowledgement feature and controls the flow of the data through flow control mechanism.

   User Datagram Protocol (UDP) – On the other hand does not provide any such features. Unlike TCP, which is connection-oriented protocol, UDP is connectionless.

Application Layer:

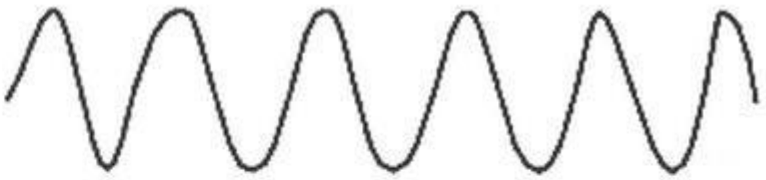
The TCP/IP specifications described a lot of applications that were at the top of the protocol stack. Some of them were TELNET, FTP, SMTP, DNS etc.

1. TELNET is a two-way communication protocol which allows connecting to a remote machine and run applications on it.
2. FTP (File Transfer Protocol) is a protocol, that allows File transfer amongst computer users connected over a network. It is reliable, simple and efficient.
3. SMTP (Simple Mail Transport Protocol) is a protocol, which is used to transport electronic mail between a source and destination, directed via a route.
4. DNS (Domain Name Server) resolves an IP address into a textual address for Hosts connected over a network.

Data Communication Fundamentals and Techniques:

Analog Signals:

An **analog** or **analogue signal** is any continuous signal for which the time varying feature (variable) of the signal is a representation of some other time varying quantity, i.e., analogous to another time varying signal. It differs from a digital signal in terms of small fluctuations in the signal which are meaningful. Analog is usually thought of in an electrical context; however, mechanical, pneumatic, hydraulic, and other systems may also convey analog signals.



Analog Signal

Digital Signals

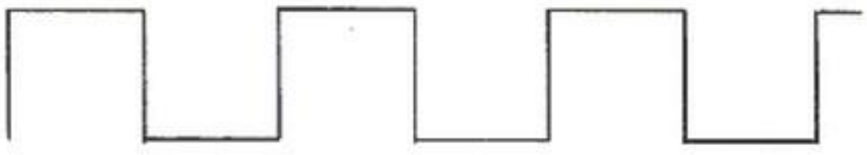
A **digital signal** is a chemical signal that is a representation of a sequence of discrete values (a quantified discrete-time signal), for example of arbitrary bit stream, or of a digitized (sampled and analog-to-digital converted) analog signal. The term digital signal can refer to

1. a continuous-time waveform signal used in any form of digital communication.

2. a pulse train signal that switches between a discrete number of voltage levels or levels of light intensity, also known as a a line coded signal, for example a signal found in digital

electronics or in serial communications using digital baseband transmission in, or a pulse code modulation (PCM) representation of a digitized analog signal.

A signal that is generated by means of a digital modulation method (digital pass band transmission), produced by a modem, is in the first case considered as a digital signal, and in the second case as converted to an analog signal.



Digital Signal

Data Rate Limits:

A very important consideration in data communications is how fast we can send data, in bits per second, over a channel. Data rate depends on three factors:

1. The bandwidth available
2. The level of the signals we use
3. The quality of the channel (the level of noise)

Noiseless channel: Nyquist bit rate

For a noiseless channel, the Nyquist bit rate formula defines the theoretical maximum bit rate

C = 2 B log2L

where, C is the channel capacity or bit rate in bps

B is the bandwidth in Hz

L is the number of signal levels used to represent data

Noisy channel: Shannon capacity

In reality, we cannot have a noiseless channel; In this case, the Shannon capacity formula is used to determine the theoretical highest data rate for a noisy channel:

C = B log2 (1+SNR)

where, C is the capacity of the channel in bps

B is the bandwidth in Hz

SNR is the signal-to-noise ratio

Performance

One important issue in networking is the performance of the network

Bandwidth

In networking, we use the term bandwidth in two contexts.

The first, bandwidth in hertz, refers to the range of frequencies in a composite signal or the range of frequencies that a channel can pass.

The second, bandwidth in bits per second, refers to the speed of bit transmission in a channel or link.

Throughput

The throughput is a measure of how fast we can actually send data through a network. Although, at first glance, bandwidth in bits per second and throughput seem the same, they are different. A link may have a bandwidth of *B* bps, but we can only send *T* bps through this link with *T* always less than *B.* In other words, the bandwidth is a potential measurement of a link; the throughput is an actual measurement of how fast we can send data. For example, we may have a link with a bandwidth of 1 Mbps, but the devices connected to the end of the link may handle only 200 kbps. This means that we cannot send more than 200 kbps through this link.

Latency (Delay)

The latency or delay defines how long it takes for an entire message to completely arrive at the destination from the time the first bit is sent out from the source. We can say that latency is made of four components: propagation time, transmission time, queuing time and processing delay.

Latency =propagation time +transmission time +queuing time + processing delay

Propagation Time

Propagation time measures the time required for a bit to travel from the source to the destination. The propagation time is calculated by dividing the distance by the propagation speed.

$$\text{Propagation time} = \frac{\textbf{Distance}}{\text{Propagation speed}}$$

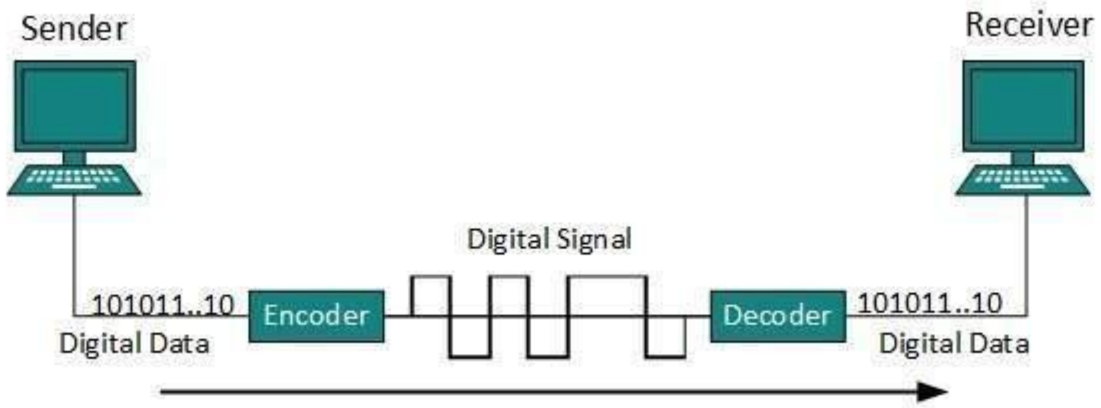
The propagation speed of electromagnetic signals depends on the medium and on the frequency of the signal For example, in a vacuum, light is propagated with a speed of 3 x 108 mfs. It is lower in air; it is much lower in cable.

Queuing Time

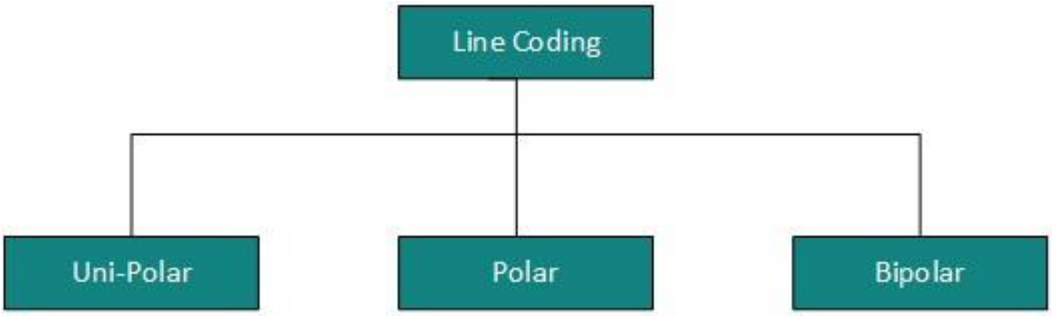
The third component in latency is the queuing time, the time needed for each intermediate or end device to hold the message before it can be processed. The queuing time is not a fixed factor; it changes with the load imposed on the network. When there is heavy traffic on the network, the queuing time increases. An intermediate device, such as a router, queues they arrived messages and processes them one by one. If there are many messages, each message will have to wait.

Line Coding Schemes:

The process for converting digital data into digital signal is said to be Line Coding. Digital data is found in binary format. It is represented (stored) internally as series of 1s and 0s.

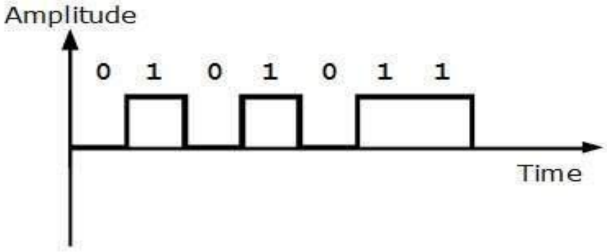


Digital signal is denoted by discreet signal, which represents digital data. There are three types of line coding schemes available:



Uni-polar Encoding:

Unipolar encoding schemes use single voltage level to represent data. In this case, to represent binary 1, high voltage is transmitted and to represent 0, no voltage is transmitted. It is also called Unipolar-Non-return-to-zero, because there is no rest condition i.e. it either represents 1 or 0.


Amplitude
0 1 0 1 0 1 1
Time

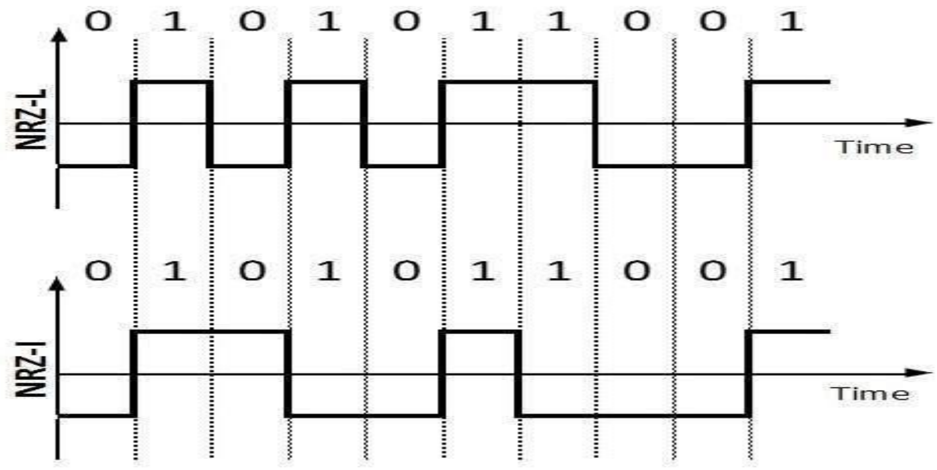
Polar Encoding:

Polar encoding scheme uses multiple voltage levels to represent binary values. Polar encodings is available in four types:

Polar Non-Return to Zero (Polar NRZ)

It uses two different voltage levels to represent binary values. Generally, positive voltage represents 1 and negative value represents 0. It is also NRZ because there is no rest condition.

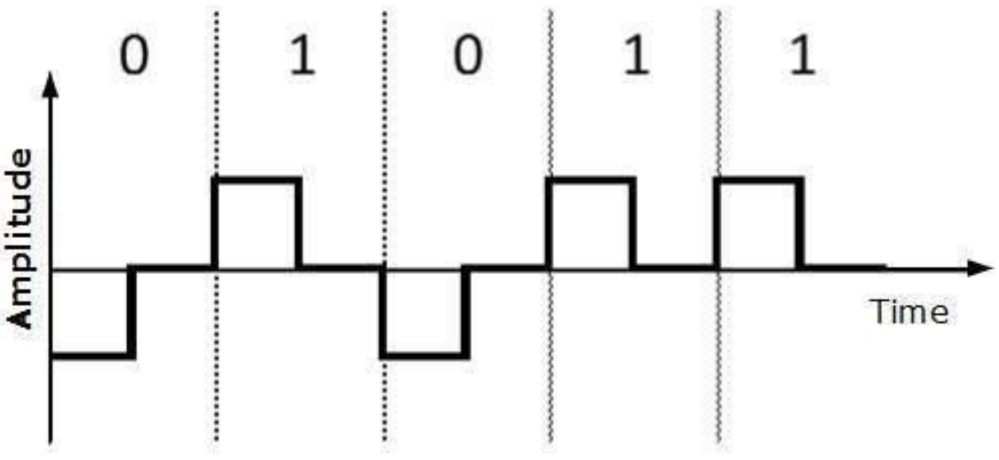
NRZ scheme has two variants: NRZ-L and NRZ-I.



NRZ-L changes voltage level at when a different bit is encountered whereas NRZ-I changes voltage when a 1 is encountered.

Return to Zero (RZ)

Problem with NRZ is that the receiver cannot conclude when a bit ended and when the next bit is started, in case when sender and receiver's clock are not synchronized.



RZ uses three voltage levels, positive voltage to represent 1, negative voltage to represent 0 and zero voltage for none. Signals change during bits not between bits.

Manchester

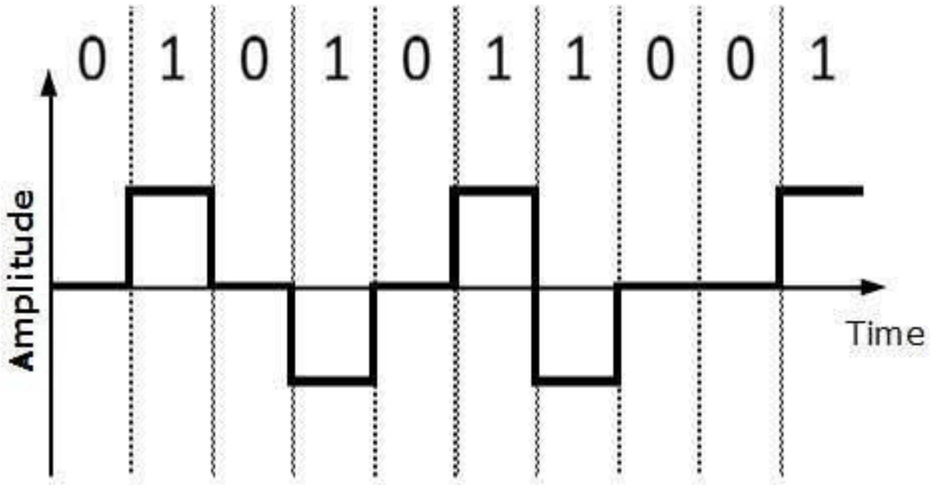
This encoding scheme is a combination of RZ and NRZ-L. Bit time is divided into two halves. It transits in the middle of the bit and changes phase when a different bit is encountered.

Differential Manchester

This encoding scheme is a combination of RZ and NRZ-I. It also transit at the middle of the bit but changes phase only when 1 is encountered.

Bipolar Encoding

Bipolar encoding uses three voltage levels, positive, negative and zero. Zero voltage represents binary 0 and bit 1 is represented by altering positive and negative voltages.



Pulse Code Modulation (PCM):

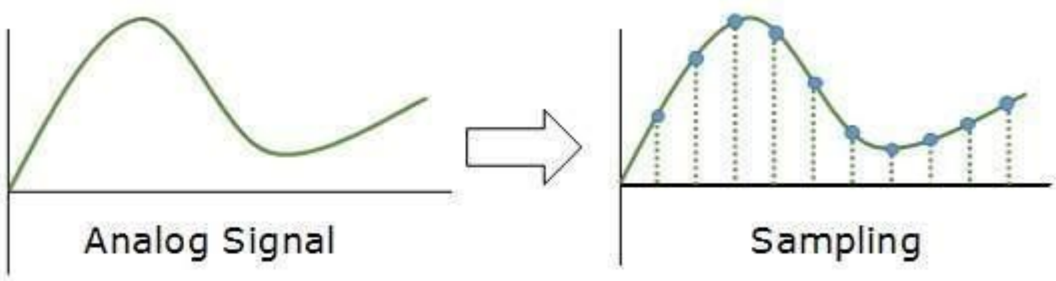
Pulse Code Modulation (PCM) is one of the most commonly used method to convert analog data into digital form. It involves three steps:

Sampling

Quantization

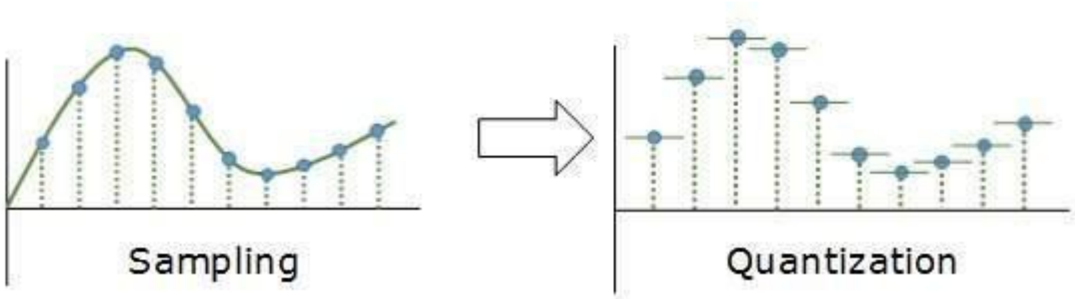
Encoding.

Sampling:



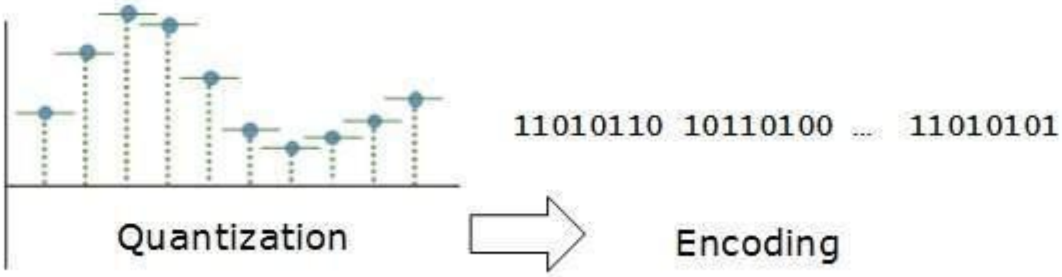
The analog signal is sampled every T interval. Most important factor in sampling is the rate at which analog signal is sampled. According to Nyquist Theorem, the sampling rate must be at least two times of the highest frequency of the signal.

Quantization:



Sampling yields discrete form of continuous analog signal. Every discrete pattern shows the amplitude of the analog signal at that instance. The quantization is done between the maximum amplitude value and the minimum amplitude value. Quantization is approximation of the instantaneous analog value.

Encoding:



In encoding, each approximated value is then converted into binary format.

Transmission Modes:

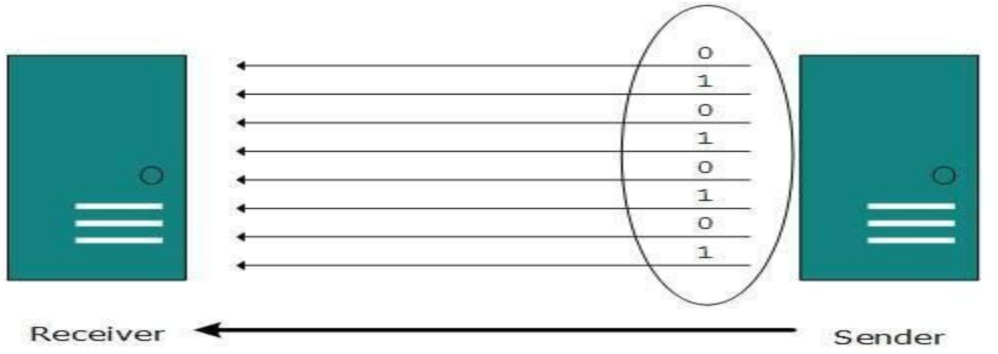
The transmission mode decides how data is transmitted between two computers.The binary data in the form of 1s and 0s can be sent in two different modes:

Parallel Transmission

Serial Transmission

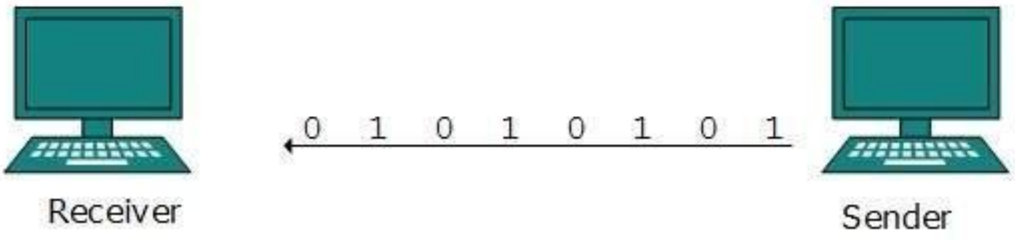
Parallel Transmission:

The binary bits are organized in-to groups of fixed length. Both sender and receiver are connected in parallel with the equal number of data lines. Both computers distinguish between high order and low order data lines. The sender sends all the bits at once on all lines. Because the data lines are equal to the number of bits in a group or data frame, a complete group of bits (data frame) is sent in one go. Advantage of Parallel transmission is high speed and disadvantage is the cost of wires, as it is equal to the number of bits sent in parallel.



Serial Transmission:

In serial transmission, bits are sent one after another in a queue manner. Serial transmission requires only one communication channel. Serial transmission can be either asynchronous or synchronous.



Asynchronous Serial Transmission:

It is named so because there is no importance of timing. Data-bits have specific pattern and they help receiver recognize the start and end data bits. For example, a 0 is prefixed on every data byte and one or more 1s are added at the end. Two continuous data-frames (bytes) may have a gap between them.

Synchronous Serial Transmission:

Timing in synchronous transmission has importance as there is no mechanism followed to recognize start and end data bits. There is no pattern or prefix/suffix method. Data bits are sent in burst mode without maintaining gap between bytes (8-bits). Single burst of data bits may contain a number of bytes. Therefore, timing becomes very important.

It is up to the receiver to recognize and separate bits into bytes.The advantage of synchronous transmission is high speed, and it has no overhead of extra header and footer bits as in asynchronous transmission.

UNIT I - POSSIBLE QUESTIONS

PART – A (20 Marks)
(Q.No 1 to 20 Online Examinations)

PART – B (2 Marks)

1. Define network.
2. Define topology.
3. What are the processes of PCM?
4. What are key elements of protocol?
5. List any 5 protocols.
6. Define Protocol.
7. What are the types of networks?
8. Define LAN.
9. Define WAN.
10. What are the Layers in ISO OSI model?

PART – C (6 Marks)

1. Explain the ISO/ OSI network model with neat sketch.
2. Discuss about digital signals in detail.
3. Explain the types of topologies.
4. Discuss about pulse code modulation
5. Describe in detail about TCP/ IP protocol suite.
6. Explain the types of transmission.
7. Explain the layered architecture.
8. Explain the types of networks.
9. Explain the overview of OSI reference Model..
10. Explain about serial transmission.

Karpagam Academy of Higher Education

Department of Computer Applications

BCA (2017-2020 Batch)

COMPUTER NETWORKS (17CAU303)

UNIT- I

S.No	Question	Option1	Option2	Option3	Option4	Answer
1	A________ is a set of devices conneted by a communication links	process	network	topology	protocol	network
2	Any device that connected to a network is referred as ________	node	client	server	link	node
3	LAN stands for _______	Local Access Network	Local Area Network	Local Architecture Network	Local Addressing Network	Local Area Network
4	______ is the set of rules.	protocol	communication	network	topology	protocol
5	Multipoint connection is also referred as _________	point-to-point	multidrop	multi node	multilink	multidrop
6	In a star topology , each device has a dedicated point to point link only to a central controller called ________	repeater	controller	hub	router	hub
7	Full duplex mode is also referred as_______	duplex	half-duplex	simplex	half-simplex	hub
8	A______connection provides a dedicated link between two devices.	point-to-point	multi-point	multidrop	physical	point-to-point
9	A ______ connection is one in which more than two specific devices share a single link	point-to-point	multi-point	multilink	dedicated	multi-point
10	In _______ topology, every device has a dedicated point-to-oint link to every other device	bus	mesh	star	ring	mesh
11	In _______ topology one long cable acts as a backbone to link all the devices in a network.	bus	mesh	star	ring	bus
12	Combination of more than one topologies is called _______	bus	mesh	hybrid	star	hybrid
13	_______ size is limited to few kilometers	MAN	LAN	WAN	Internet	LAN
14	NIC stands for ______	Network Interface Card	Network Information Centre	Network Interface Centre	Network Information Card	Network Interface Card
15	There are _____ layers in ISO OSI model	4	5	6	7	7
16	The physical layer coordinates the functions required to carry a _______ over a physical medium	frame	packet	segment	bit stream	bitstream
17	The________ layer coordinates the functions required to carry a bitstream over a physical medium.	datalink	physical	application	session	physical

18	Hop to hop delivery is done by the __________	session layer	datalink layer	network layer	transport layer	datalink layer
19	The __________layer is responsible for process to process delivery.	physical	presentation	network	transport	transport
20	The ________layer is responsible for dialog control and synchronization.	transport	session	application	presentation	session
21	The ______ layer is responsible for the souce to destination delivery of a packets.	physical	network	transport	presentation	network
22	The ________ layer is responsible for process to process delivery.	transport	session	application	presentation	transport
23	The _____ layer is concerned with the syntax and semantics of the information exchanged between two	physical	network	transport	presentation	physical
24	There are _____ layers in TCP/IP Protocol Suite	4	5	6	7	4
25	TCP/IP is a _______protocol.	hyper text	transfer	internet	hierarchical	hierarchical
26	TCP stands for ______	Transfer Control Protocol	Transmission Control Protocol	Transport Control Protocol		
27	OSI stands for__________	open systems interconnection	open system internetworking	open symantic interconnection	open system internet	open systems interconnection
28	Network layer delivers data in the form of_______	frame	bits	data	packet	packet
29	Session layer provides_________ services.	one	two	three	four	two
30	ARP stands for _______	Address Resolution Protocol	Access Resolution Prototype	Access Resource Protocol	Address Resolution Prototype	Address Resolution Protocol
31	_______ is used to associate a logical address with a physical address	ARP	RARP	ICMP	IGMP	ARP
32	RARP stands for _______	Reverse Address Resolution Protocol	Revised Access Resolution Prototype	Repeat Access Resource Protocol	Random Address Resolution Prototype	Reverse Address Resolution Protocol
33	_______ allows a host to discove its Internet address when it knows only its physical address	ARP	RARP	ICMP	IGMP	RARP
34	ICMP stands for ________	Interface Control Message Protocol	Internet Control Message Protocol	Interface Control Medium Protocol	Internet Control Medium Protocol	Internet Control Message Protocol
35	_________ sends query and error reporting messages	ARP	RARP	ICMP	IGMP	ICMP
36	IGMP stands for ________	Interface Group Message Protocol	Internet Group Message Protocol	Interface Gateway Medium Protocol	Internet Gateway Medium Protocol	Internet Group Message Protocol
37	_________ provides support for newer applications such as voice over Internet	SCTP	SMTP	ICMP	IGMP	SCTP
38	UDP _________	user data protocol	user datagram protocol	user defined protocol	user dataframe protocol	user datagram protocol
39	FTP___________	file transmit protocol	file transmission protocol	file transfer protocol	flip transfer protocol	file transfer protocol
40	SMTP____________	single mail transfer protocol	simple mail transfer protocol	simple mail transmission protocol	single mail transmit protocol	simple mail transfer protocol

41	Complete a cycle is called as ________	period	frequency	non periodic	periodic	period
42	A MAN is a network with a size between a _________ and ___________.	WAN and LAN	WAN or LAN	LAN	WAN	WAN and LAN
43	The_________layer is responsible for providing services to the user.	presentation	datalink	application	network	application
44	The ________ layer is responsible for translation, compression encryption.	transport	data link	presentation	application	presentation
45	___________does not define any specific protocol.	TCP	HTTP	TCP/IP	SMTP	TCP/IP
46	The TCP/IP protocol suite was developed prior to the___________model.	OSI	ISO	TCP	IP	OSI
47	How many sampling methods are available?	2	3	4	5	3
48	PCM stands for______	Pulse Coding Modulation	Pulse Coded Modulation	Pulse Code Modulation	Pulse Card Modulation	Pulse Code Modulation
49	The _______ process is referred as pulse amplitude modulation	sampling	quantizing	encoding	decoding	sampling
50	PAM stands for _____	Pulse Amplitude Modulation	Pulse Amplified Modulation	Pulse Amplify Modulation	Pulse Amplifing Modulation	Pulse Amplitude Modulation
51	The first step in PCM is ______	sampling	quantizing	encoding	decoding	sampling
52	The signals which are obtained by encoding each quantized signal into a digital word is called as	PAM signal	PCM Signal	FM signal	sampling & quantization	PCM Signal
53	_______ prvides synchronization without increasing the number of bits	sampling	quantizing	encoding	scrambling	scrambling

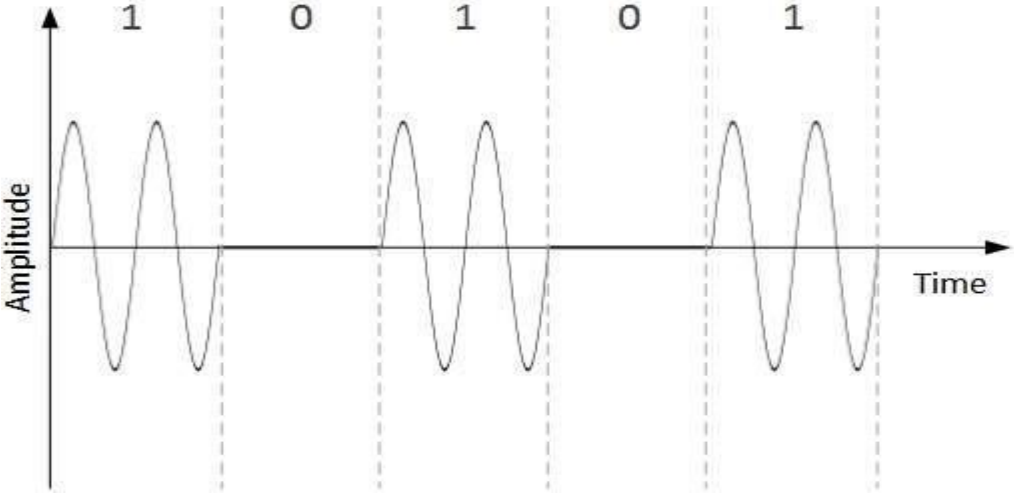
Digital-to-Analog Modulation:

When data from one computer is sent to another via some analog carrier, it is first converted into analog signals. Analog signals are modified to reflect digital data.

An analog signal is characterized by its amplitude, frequency, and phase. There are three kinds of digital-to-analog conversions:

- **Amplitude Shift Keying**

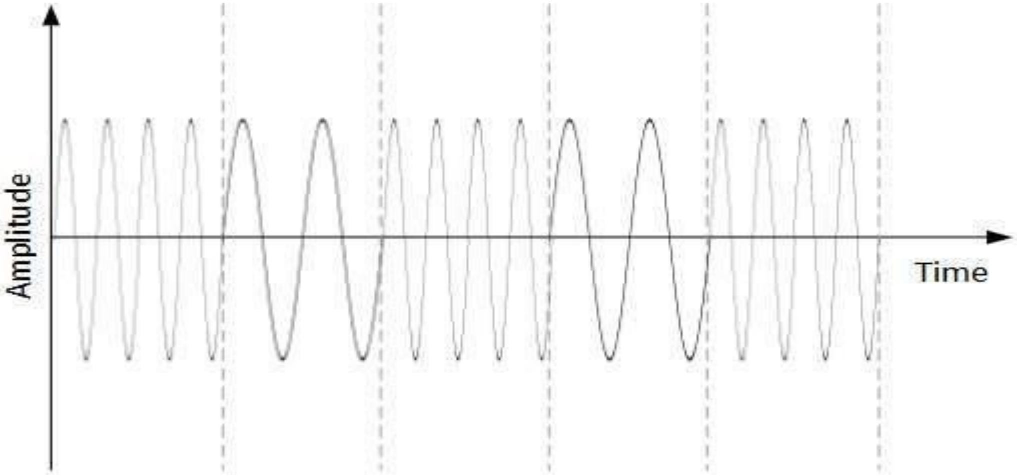
  In this conversion technique, the amplitude of analog carrier signal is modified to reflect binary data.



  When binary data represents digit 1, the amplitude is held; otherwise it is set to 0. Both frequency and phase remain same as in the original carrier signal.

- **Frequency Shift Keying**

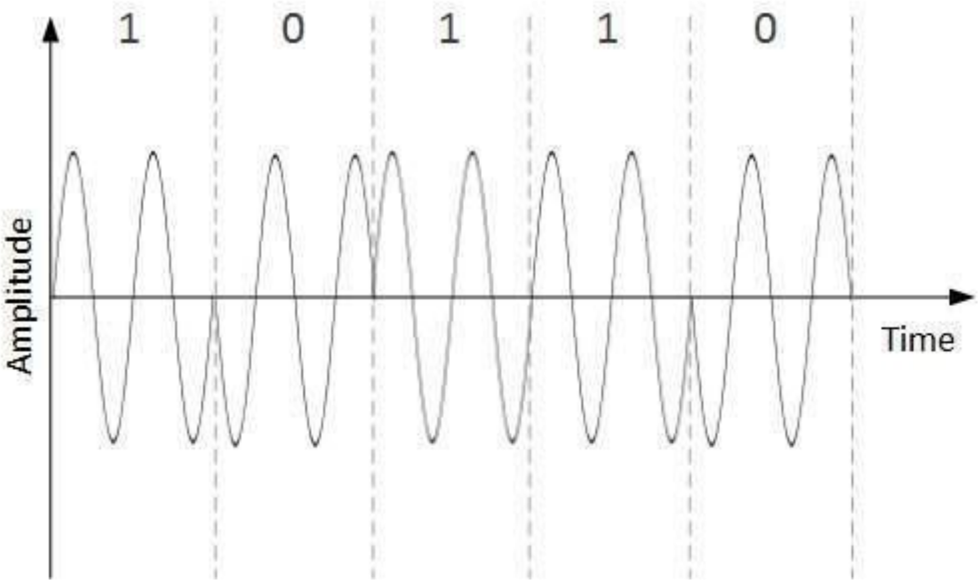
  In this conversion technique, the frequency of the analog carrier signal is modified to reflect binary data.



  This technique uses two frequencies, f1 and f2. One of them, for example f1, is chosen to represent binary digit 1 and the other one is used to represent binary digit 0. Both amplitude and phase of the carrier wave are kept intact.

- **Phase Shift Keying**

  In this conversion scheme, the phase of the original carrier signal is altered to reflect the binary data.



  When a new binary symbol is encountered, the phase of the signal is altered. Amplitude and frequency of the original carrier signal is kept intact.

- **Quadrature Phase Shift Keying**

  QPSK alters the phase to reflect two binary digits at once. This is done in two different phases. The main stream of binary data is divided equally into two sub-streams. The serial data is converted in to parallel in both sub-streams and then each stream is converted to digital signal using NRZ technique. Later, both the digital signals are merged together.

Multiplexing Technique:

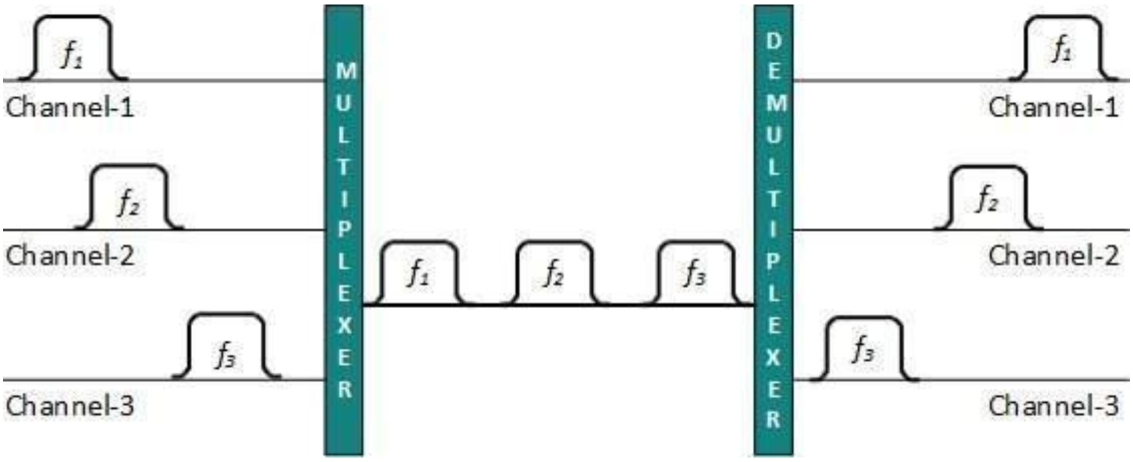
Multiplexing is a technique by which different analog and digital streams of transmission can be simultaneously processed over a shared link. Multiplexing divides the high capacity medium into low capacity logical medium which is then shared by different streams.

Communication is possible over the air (radio frequency), using a physical media (cable), and light (optical fiber). All mediums are capable of multiplexing.

When multiple senders try to send over a single medium, a device called Multiplexer divides the physical channel and allocates one to each. On the other end of communication, a De-multiplexer receives data from a single medium, identifies each, and sends to different receivers.

Frequency Division Multiplexing (FDM):

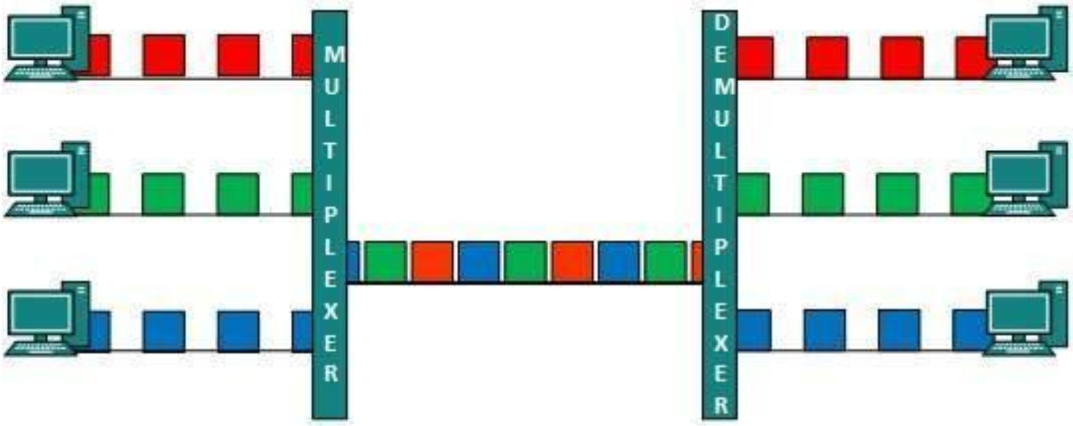
When the carrier is frequency, FDM is used. FDM is an analog technology. FDM divides the spectrum or carrier bandwidth in logical channels and allocates one user to each channel. Each user can use the channel frequency independently and has exclusive access of it. All channels are divided in such a way that they do not overlap with each other. Channels are separated by guard bands. Guard band is a frequency which is not used by either channel.



Time Division Multiplexing (TDM):

TDM is applied primarily on digital signals but can be applied on analog signals as well. In TDM the shared channel is divided among its user by means of time slot. Each user can transmit data within the provided time slot only. Digital signals are divided in frames, equivalent to time slot i.e. frame of an optimal size which can be transmitted in given time slot.

TDM works in synchronized mode. Both ends, i.e. Multiplexer and De-multiplexer are timely synchronized and both switch to next channel simultaneously.



When channel A transmits its frame at one end, the De-multiplexer provides media to channel A on the other end. As soon as the channel A's time slot expires, this side switches to channel B. On the other end, the De-multiplexer works in a synchronized manner and provides media to channel B. Signals from different channels travel the path in interleaved manner.

Transmission Media:

For any networking to be effective, raw stream of data is to be transported from one device to other over some medium. Various transmission media can be used for transfer of data. These transmission media may be of two types −

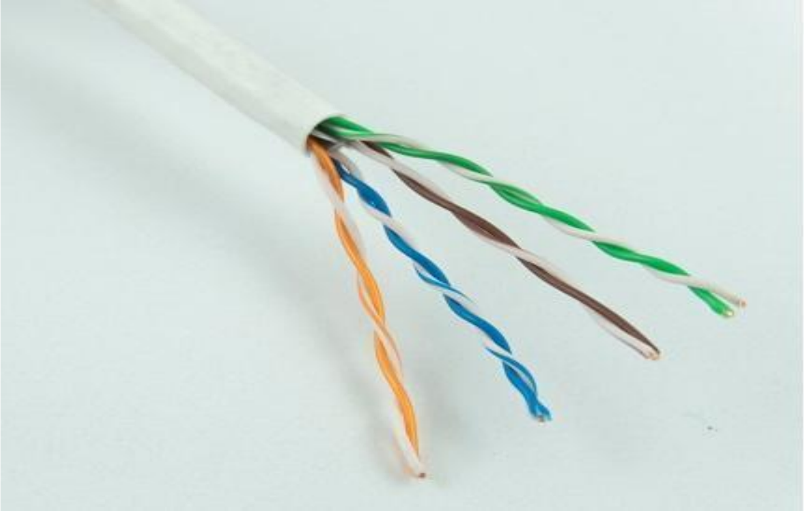
1. **Guided** − In guided media, transmitted data travels through cabling system that has a fixed path. For example, copper wires, fiber optic wires, etc.
2. **Unguided** − In unguided media, transmitted data travels through free space in form of electromagnetic signal. For example, radio waves, lasers, etc.

Each transmission media has its own advantages and disadvantages in terms of bandwidth, speed, delay, cost per bit, ease of installation and maintenance, etc.

Guided Media:

Twisted Pair Cable:

Copper wires are the most common wires used for transmitting signals because of good performance at low costs. They are most commonly used in telephone lines. However, if two or more wires are lying together, they can interfere with each other's signals. To reduce this electromagnetic interference, pair of copper wires are twisted together in helical shape like a DNA molecule. Such twisted copper wires are called **twisted pair**. To reduce interference between nearby twisted pairs, the twist rates are different for each pair.



Up to 25 twisted pair are put together in a protective covering to form twisted pair cables that are the backbone of telephone systems and Ethernet networks.

Advantages of twisted pair cable:

Twisted pair cable are the oldest and most popular cables all over the world. This is due to the many advantages that they offer −

- Trained personnel easily available due to shallow learning curve

- Can be used for both analog and digital transmissions
- Least expensive for short distances
- Entire network does not go down if a part of network is damaged

Disadvantages of twisted pair cable:

With its many advantages, twisted pair cables offer some disadvantages too −

- Signal cannot travel long distances without repeaters
- High error rate for distances greater than 100m
- Very thin and hence breaks easily
- Not suitable for broadband connections

Shielding twisted pair cable:

To counter the tendency of twisted pair cables to pick up noise signals, wires are shielded in the following three ways −

- Each twisted pair is shielded.
- Set of multiple twisted pairs in the cable is shielded.
- Each twisted pair and then all the pairs are shielded.

Such twisted pairs are called **shielded twisted pair (STP) cables**. The wires that are not shielded but simply bundled together in a protective sheath are called **unshielded twisted pair (UTP) cables**. These cables can have maximum length of 100 metres.

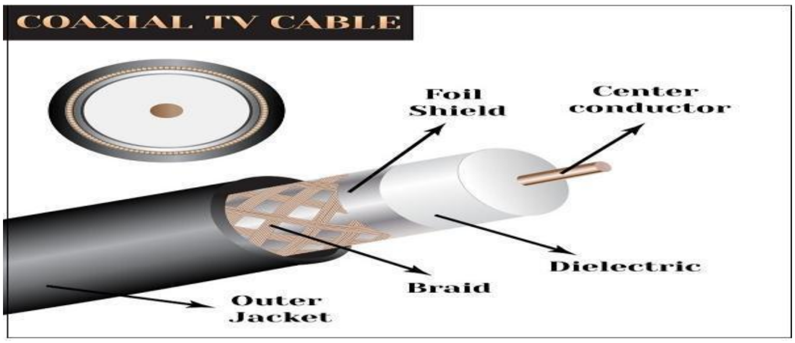
Shielding makes the cable bulky, so UTP are more popular than STP. UTP cables are used as the last mile network connection in homes and offices.

Coaxial Cable:

Coaxial cables are copper cables with better **shielding** than twisted pair cables, so that transmitted signals may travel longer distances at higher speeds. A coaxial cable consists of these layers, starting from the innermost −

- Stiff copper wire as **core**
- **Insulating material** surrounding the core
- Closely woven braided mesh of **conducting material** surrounding the **insulator**
- Protective **plastic sheath** encasing the wire

Coaxial cables are widely used for **cable TV** connections and **LANs**.



Advantages of Coaxial Cables

These are the advantages of coaxial cables −

- Excellent noise immunity
- Signals can travel longer distances at higher speeds, e.g. 1 to 2 Gbps for 1 Km cable
- Can be used for both analog and digital signals
- Inexpensive as compared to fibre optic cables
- Easy to install and maintain

Disadvantages of Coaxial Cables

These are some of the disadvantages of coaxial cables −

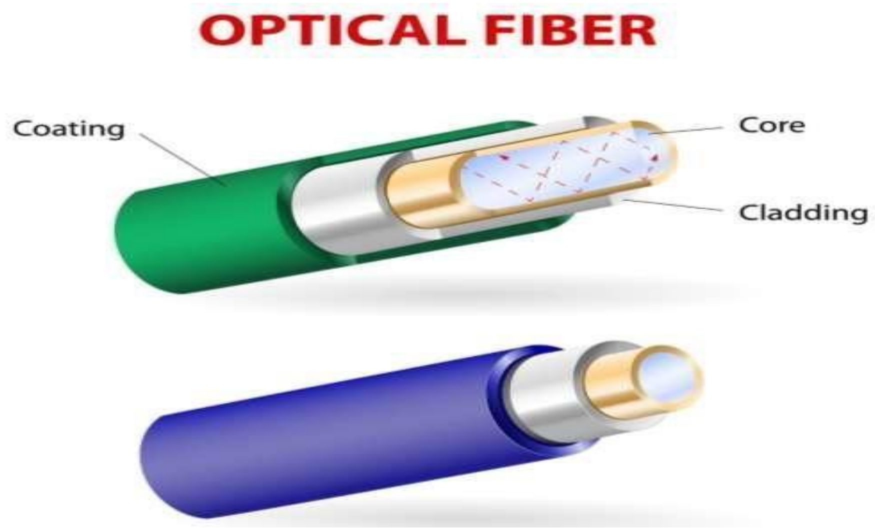
- Expensive as compared to twisted pair cables
- Not compatible with twisted pair cables

Optical Fiber

Thin glass or plastic threads used to transmit data using light waves are called **optical fiber**. Light Emitting Diodes (LEDs) or Laser Diodes (LDs) emit light waves at the **source**, which is read by a **detector** at the other end. **Optical fiber cable** has a bundle of such threads or fibers bundled together in a protective covering. Each fiber is made up of these three layers, starting with the innermost layer −

- **Core** made of high quality **silica glass** or **plastic**
- **Cladding** made of high quality **silica glass** or **plastic**, with a lower refractive index than the core
- Protective outer covering called **buffer**

Note that both core and cladding are made of similar material. However, as **refractive index** of the cladding is lower, any stray light wave trying to escape the core is reflected back due to **total internal reflection**.



Optical fiber is rapidly replacing copper wires in telephone lines, internet communication and even cable TV connections because transmitted data can travel very long distances without weakening. **Single node** fiber optic cable can have maximum segment length of 2 kms and bandwidth of up to 100 Mbps. **Multi-node** fiber optic cable can have maximum segment length of 100 kms and bandwidth up to 2 Gbps.

Advantages of Optical Fiber

Optical fiber is fast replacing copper wires because of these advantages that it offers −

- High bandwidth
- Immune to electromagnetic interference
- Suitable for industrial and noisy areas
- Signals carrying data can travel long distances without weakening

Disadvantages of Optical Fiber

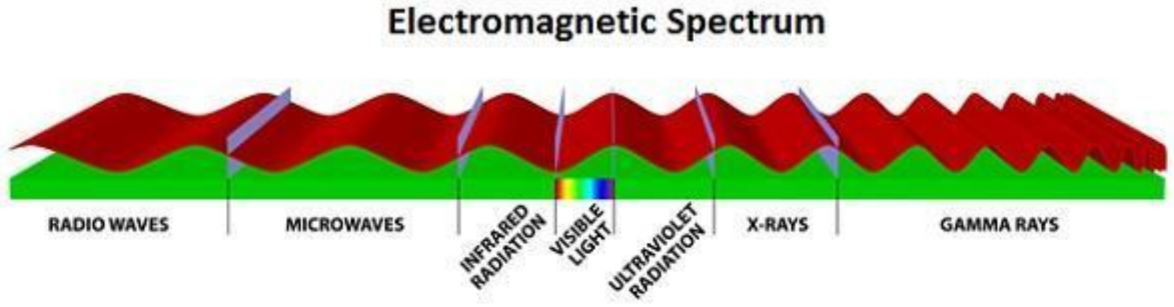
Despite long segment lengths and high bandwidth, using optical fiber may not be a viable option for every one due to these disadvantages −

- Optical fiber cables are expensive
- Sophisticated technology required for manufacturing, installing and maintaining optical fiber cables
- Light waves are unidirectional, so two frequencies are required for full duplex transmission

Unguided Media:

Infrared:

Low frequency infrared waves are used for very short distance communication like TV remote, wireless speakers, automatic doors, hand held devices etc. Infrared signals can propagate within a room but cannot penetrate walls. However, due to such short range, it is considered to be one of the most secure transmission modes.



Radio Wave:

Transmission of data using radio frequencies is called **radio-wave transmission**. We all are familiar with radio channels that broadcast entertainment programs. Radio stations transmit radio waves using **transmitters**, which are received by the receiver installed in our devices.

Both transmitters and receivers use antennas to radiate or capture radio signals. These radio frequencies can also be used for **direct voice communication** within the **allocated range**. This range is usually 10 miles.

Advantages of Radio Wave

These are some of the advantages of radio wave transmissions −

- Inexpensive mode of information exchange
- No land needs to be acquired for laying cables
- Installation and maintenance of devices is cheap

Disadvantages of Radio Wave

These are some of the disadvantages of radio wave transmissions −

- Insecure communication medium
- Prone to weather changes like rain, thunderstorms, etc.

Networks Switching Techniques and Access Mechanisms:

Switching:

Switching is process to forward packets coming in from one port to a port leading towards the destination. When data comes on a port it is called ingress, and when data leaves a port or goes out it is called egress. A communication system may include number of switches and nodes. At broad level, switching can be divided into two major categories:

- **Connectionless:** The data is forwarded on behalf of forwarding tables. No previous handshaking is required and acknowledgements are optional.
- **Connection Oriented:** Before switching data to be forwarded to destination, there is a need to pre-establish circuit along the path between both endpoints. Data is then

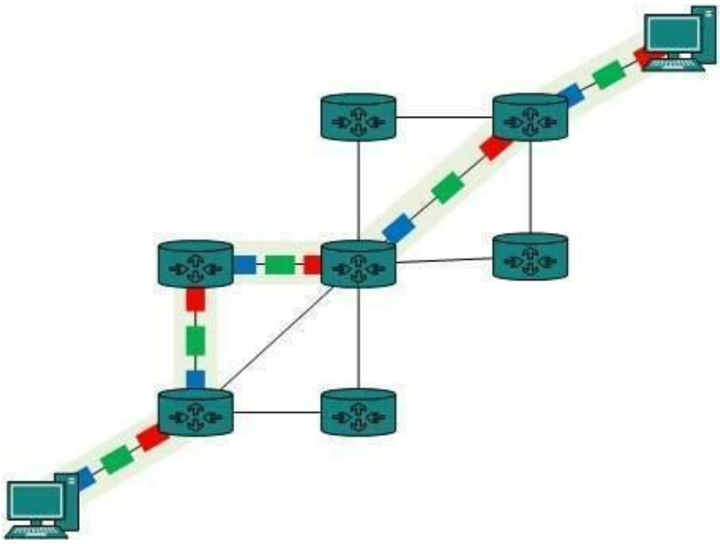
forwarded on that circuit. After the transfer is completed, circuits can be kept for future use or can be turned down immediately.

Circuit Switching:

When two nodes communicate with each other over a dedicated communication path, it is called circuit switching. There 'is a need of pre-specified route from which data will travels and no other data is permitted. In circuit switching, to transfer the data, circuit must be established so that the data transfer can take place.

Circuits can be permanent or temporary. Applications which use circuit switching may have to go through three phases:

- Establish a circuit
- Transfer the data
- Disconnect the circuit



Circuit switching was designed for voice applications. Telephone is the best suitable example of circuit switching. Before a user can make a call, a virtual path between caller and callee is established over the network.

Advantages of Circuit Switching:

Circuit switching provides these advantages over other switching techniques −

- Once path is set up, the only delay is in data transmission speed
- No problem of congestion or garbled message

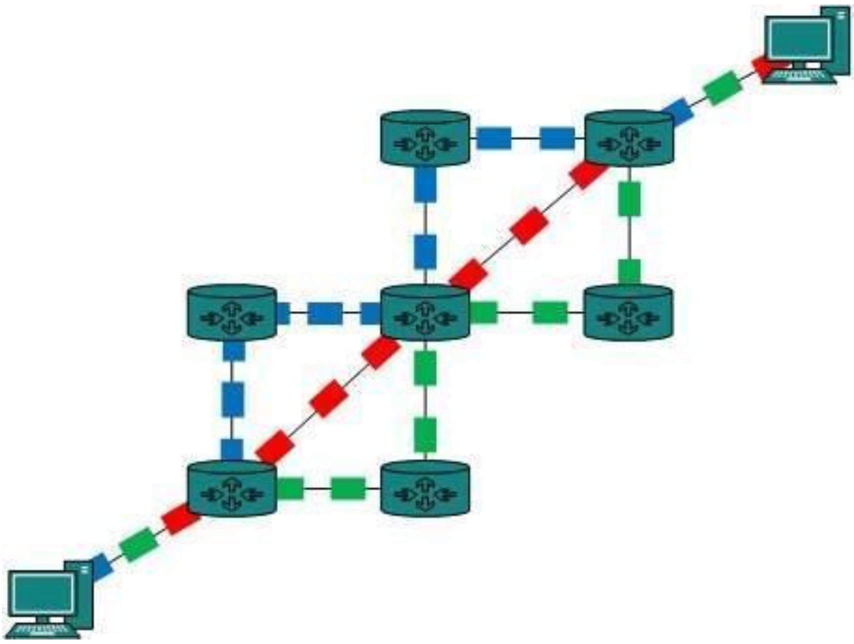
Disadvantages of Circuit Switching

Circuit switching has its disadvantages too −

- Long set up time is required
- A request token must travel to the receiver and then acknowledged before any transmission can happen
- Line may be held up for a long time

Packet Switching:

Shortcomings of message switching gave birth to an idea of packet switching. The entire message is broken down into smaller chunks called packets. The switching information is added in the header of each packet and transmitted independently. It is easier for intermediate networking devices to store small size packets and they do not take much resources either on carrier path or in the internal memory of switches.



Packet switching enhances line efficiency as packets from multiple applications can be multiplexed over the carrier. The internet uses packet switching technique. Packet switching enables the user to differentiate data streams based on priorities. Packets are stored and forwarded according to their priority to provide quality of service.

Connectionless Datagram Switching:

Connectionless datagram switching is a packet switching technology by which each packet, now called a datagram, is treated as a separate entity. Each packet is routed independently through the network. Therefore packets contain a header with the full information about the destination. The intermediate nodes examine the header of a packet and select an appropriate link to another node which is nearer to the destination. In this system, the packets do not follow a pre-established route, and the intermediate nodes do not require prior knowledge of the routes that will be used.

The individual packets which form a data stream may follow different paths between the source and the destination. As a result, the packets may arrive at the destination out of order. When this occurs, the packets will have to be reassembled to form the original message.

Because each packet is switched independently, there is no need for connection setup and no need to dedicate bandwidth in the form of a circuit.

Datagram packet switches use a variety of techniques to forward traffic; they are differentiated by how long it takes the packet to pass through the switch and their ability to filter out corrupted packets.

There are three primary types of datagram packet switches:

- **Store and forward**: buffers data until the entire packet is received and checked for errors. This prevents corrupted packets from propagating throughout the network but increases switching delay.
- **Fragment free**: filters out most error packets but doesn't necessarily prevent the propagation of errors throughout the network. It offers faster switching speeds and lower delay than store-and-forward mode.
- **Cut through**:does not filter errors; it switches packets at the highest throughput, offering the least forwarding delay.

A datagram network is a best effort network. Delivery is not guaranteed. Reliable delivery must be provided by the end systems (i.e. user's computers) using additional protocols.

The most common datagram network is the Internet, which uses the IP network protocol. Applications which do not require more than a best effort service can be supported by direct use of packets in a datagram network, using the User Datagram Protocol (UDP) transport protocol. Applications like voice and video communications and notifying messages to alert a user that she/he has received new email are using UDP. Applications like e-mail, web browsing and file upload and download need reliable communications, such as guaranteed delivery, error control and sequence control. This reliability ensures that all the data is received in the correct order without errors. It is provided by a protocol such as the Transmission Control Protocol (TCP) or the File Transfer Protocol (FTP).

Virtual Circuit Switching:

Virtual circuit switching is a packet switching methodology whereby a path is established between the source and the final destination through which all the packets will be routed during a call. This path is called a virtual circuit because to the user, the connection appears to be a dedicated physical circuit. However, other communications may also be sharing the parts of the same path.

Before the data transfer begins, the source and destination identify a suitable path for the virtual circuit. All intermediate nodes between the two points put an entry of the routing in their routing table for the call. Additional parameters, such as the maximum packet size, are also exchanged between the source and the destination during call setup. The virtual circuit is cleared after the data transfer is completed. Virtual circuit packet switching is connection oriented. This is in contrast to datagram switching, which is a connection less packet switching methodology.

Advantages:

- Packets are delivered in order, since they all take the same route;
- The overhead in the packets is smaller, since there is no need for each packet to contain the full address;
- The connection is more reliable, network resources are allocated at call setup so that even during times of congestion, provided that a call has been setup, the subsequent packets should get through;
- Billing is easier, since billing records need only be generated per call and not per packet.

Disadvantages:

- The switching equipment needs to be more powerful, since each switch needs to store details of all the calls that are passing through it and to allocate capacity for any traffic that each call could generate;
- Resilience to the loss of a trunk is more difficult, since if there is a failure all the calls must be dynamically reestablished over a different route.

Examples of virtual circuit switching are X.25 and Frame Relay.

Dial-up Modems:

Traditional **modems** used on **dial-up networks** convert data between the analog form used on telephone lines and the digital form used on **computers**. An external **dial-up modem** plugs into a **computer** at one end and a telephone line on the other end.

Traditional telephone lines can carry frequencies between 300 and 3300 Hz, giving them a bandwidth of 3000 Hz. All this range is used for transmitting voice, where a great deal of interference and distortion can be accepted without loss of intelligibility.

The term modem is a composite word that refers to the two functional entities that make up the device: a signal modulator and a signal demodulator. A modulator creates a band pass analog signal from binary data. A demodulator recovers the binary data from the modulated signal.

Modem stands for modulator/demodulator:

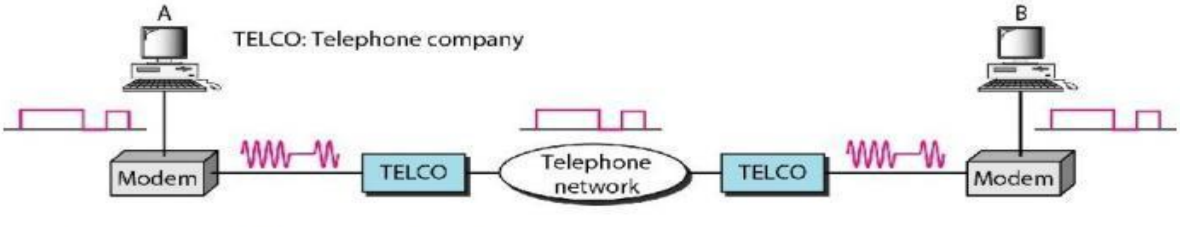


Figure Modulation/Demodulation

Digital Subscriber Line:

Digital Subscriber Line (DSL) is a high-speed Internet service for homes and businesses that competes with cable and other forms of broadband Internet. DSL provides high-speed networking over ordinary phone lines using broadband modem technology. The technology behind DSL enables Internet and telephone service to work over the same phone line without requiring customers to disconnect either their voice or Internet connections.

DSL Speed

Basic DSL supports maximum download data rates ranging between 1.544 Mbps and 8.448 Mbps. Actual speeds vary in practice depending on the quality of the copper phone line installation involved. The length of the phone line needed to reach the service provider's premise equipment (sometimes called the "central office") also can limit the maximum speed a DSL installation supports.

Symmetric vs. Asymmetric DSL

Most types of DSL service are asymmetric and symmetric

- Asymmetric is also known as ADSL. ADSL offers higher download speeds than upload speeds, a tradeoff that most residential providers make to better match up with the needs of typical households who generally do much more downloading.
- Symmetric DSL maintains equal data rates for both uploads and downloads.

Residential DSL Service

Well-known DSL providers in the United States include AT&T (Uverse), Verizon, and Frontier Communications.

Many smaller regional providers also offer DSL. Customers subscribe to a DSL service plan and pay a monthly or yearly subscription and must also agree to the provider's terms of service. Most providers supply compatible DSL modem hardware to their customers if needed, although the hardware is generally available through retailers.

Business DSL Service

Besides its popularity in homes, many businesses also rely on DSL for their Internet service. Business DSL differs from residential DSL in several key respects:

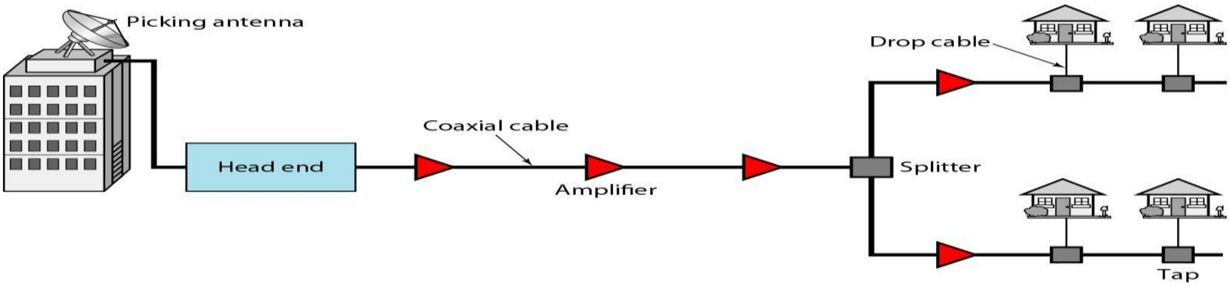
- Symmetric DSL is typically used as businesses tend to generate much higher volumes of outgoing traffic than a typical home

- Providers often sell higher tiers of service to their customers including higher data rate plans, premier customer support options or bundling of other products

CABLE TV NETWORKS:

The cable TV network started as a video service provider, but it has moved to the business of Internet access. In this section, we discuss cable TV networks per se; in Section 9.5 we discuss how this network can be used to provide high-speed access to the Internet.

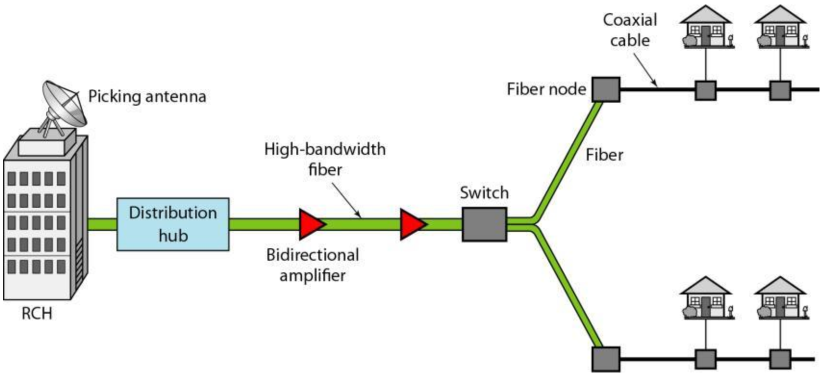
Traditional cable TV network



Communication in the traditional cable TV network is unidirectional

The cable TV office, called the head end, receives video signals from broadcasting stations and feeds the signals into coaxial cables. The signals became weaker and weaker with distance, so amplifiers were installed through the network to renew the signals. There could be up to 35 amplifiers between the head end and the subscriber premises. At the other end, splitters split the cable, and taps and drop cables make the connections to the subscriber premises.

Hybrid fiber-coaxial (HFC) network

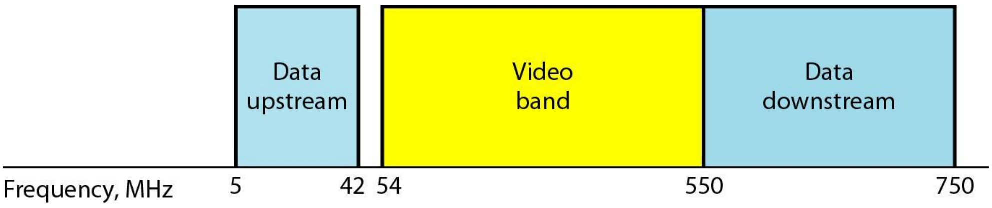


Communication in an HFC cable TV network can be bidirectional.

The second generation of cable networks is called a hybrid fiber-coaxial (HFC) network. The network uses a combination of fiber-optic and coaxial cable. The transmission medium from the cable TV office to a box, called the fiber node, is optical fiber; from the fiber node through the neighborhood and into the house is still coaxial cable.

Cable companies are now competing with telephone companies for the residential customer who wants high-speed data transfer. In this section, we briefly discuss this technology.

Division of coaxial cable band by CATV

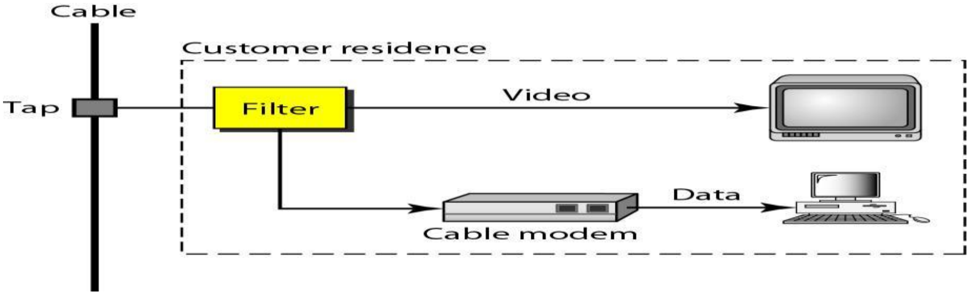


Downstream data are modulated using the 64-QAM modulation technique. The theoretical downstream data rate is 30 Mbps.

Upstream data are modulated using the QPSK modulation technique. The theoretical upstream data rate is 12 Mbps.

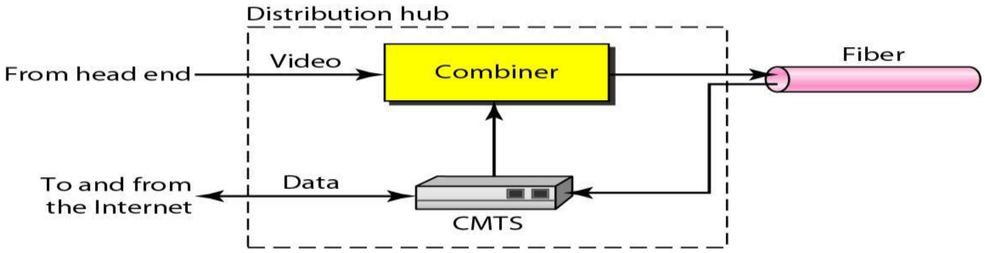
Cable modem (CM)

The cable modem (CM) is installed on the subscriber premises. It is similar to an ADSL modem.



Cable modem transmission system (CMTS)

The cable modem transmission system (CMTS) is installed inside the distribution hub by the cable company. It receives data from the Internet and passes them to the combiner, which sends them to the subscriber. The CMTS also receives data from the subscriber and passes them to the Internet.


Distribution hub
From head end
Video
Combiner
Fiber
To and from the Internet
Data
CMTS

KarpagamAcademy of Higher Education

(Established Under Section 3 of UGC Act 1956) Eachanari Post,
Coimbatore – 641 021. INDIA
Phone : 0422-2611146, 2611082 Fax No : 0422 -2611043

Enable | Enlighten | Enrich
(Deemed to be University)
(Under Section 3 of UGC Act 1956)

DEPARTMENT OF COMPUTER APPLICATIONS

BCA (2017-2020 BATCH)

COURSE NAME: COMPUTER NETWORKS **COURSE CODE: 17CAU303**

UNIT II - POSSIBLE QUESTIONS

PART – A (20 Marks)

(Q.No 1 to 20 Online Examinations)

PART – B

(Each question carries two marks)

1. List the advantages of Optic Fiber Cable.
2. What is Multiplexing?
3. Define transmission medium.
4. Define Radio Waves.
5. What is switching?
6. Differentiate analog and digital signal.
7. What is demultiplexing?
8. Define TDM.
9. Define digital data.
10. Define analog signal.

PART – C

(Each question carries six marks)

1. Describe about the Frequency Division Multiplexing.
2. Explain about fiber optic media for communication.
3. Explain about time division multiplexing with neat diagram.
4. Write about circuit switched networks.
5. Illustrate the Digital Subscriber Line.
6. Elucidate the Virtual Circuit Network in detail.
7. Describe about the time division multiplexing with neat diagram.
8. Explain in detail about the datagram networks.
9. Explain the twisted pair cable and coaxial cable in detail.
10. Write about cable TV for data transfer in detail.

Karpagam Academy of Higher Education

Department of Computer Applications

BCA (2017-2020 Batch)

COMPUTER NETWORKS (17CAU303)

UNIT- II

S.No	Question	Option1	Option2	Option3	Option4	Answer
1	_________ is a set of techniques that allows the simultaneous transmission of multiple signals across a	Multiplexing	Demultiplexing	Interleaving	Synchronizing	Multiplexing
2	ASK stands for _______	Amplifier Shift Keying	Amplitude Shift Keying	Analog Shift Keying	Amplify Shift Keying	Amplitude Shift Keying
3	FSK stands for ______	Frame Shift Keying	Functional Shift Keying	Frequency Shift Keying	Final Shift Keying	Frequency Shift Keying
4	PSK stands for _____	Phase Shift Keying	Period Shift Keying	Performance Shift Keying	Page Shift Keying	Phase Shift Keying
5	QAM stands for ______	Quadrature Amplifier Modulation	Quadrature Amplitude	Quadrature Analog Modulation	Quadrature Amplify Modulation	Quadrature Amplitude Modulation
6	________ conversion is the process of changing one of the characteristics of an analog signal based on the	Analog to anlog	Digital to digital	Analog to digital	Digital to analog	Digital to analog
7	A _______ is a device that selects one of several analog or digital input signals and forwards the selected input	demultiplexer	multiplexer	converter	inverter	multiplexer
8	A _________ is a device that takes a single input line and routes it to one of several digital output lines	demultiplexer	multiplexer	converter	inverter	demultiplexer
9	The word ______ refers to the portion of a link that carries a transmission between a given pair of lines	path	link	channel	node	channel
10	FDM stands for ________	Frame Division Multiplexing	Functional Division Multiplexing	Frequency Division Multiplexing	Factor Division Multiplexing	Frequency Division Multiplexing
11	________ is a analog multiplexing technique that combines analog signal	TDM	FDM	WDM	ADM	FDM
12	WDM stands for _______	Work Division Multiplexing	Wavelength Division Multiplexing	Weight Division Multiplexing	Web Division Multiplexing	Wavelength Division Multiplexing
13	________ is designed to use the high-data-rate capability of fiber optic cable	TDM	FDM	WDM	ADM	WDM
14	TDM stands for _______	Time Division Multiplexing	Type Division Multiplexing	Test Division Multiplexing	Transmission Division Multiplexing	Time Division Multiplexing
15	___________ is a digital multiplexing technique	TDM	FDM	WDM	ADM	TDM
16	Multiplexing is used in _______	Packet switching	Circuit switching	Data switching	datagram switching	Circuit switching
17	In multiplexing, channels are separated by unused strips of bandwidth guard bands - to prevent __________	Synchronization	Overlapping	random motion of electrons	interleaving	Overlapping

18	Frequency difference between WDM and FDM is _______	very high	very low	zero	infinity	very high
19	Transmission media are actually located below the __________ layer.	application	presentation	physical	data link	physical
20	Transmission media are directly controlled by the _________	physical layer	data link layer	network layer	session layer	physical layer
21	Optical fibers use reflection to guide light through a _________	channel	metal wire	light	plastic	channel
22	Which transmission media has the highest transmission speed in a network?	coaxial cable	twisted pair cable	fiber optic cable	electrical cable	optical fiber cable
23	__________ is a cable made up of glass or plastics that transmits the signlas in the form of light	coaxial cable	twisted pair cable	fiber optic cable	electrical cable	optical fiber cable
24	_________ cable consists of two insulated copper wires twisted together.	coaxial cable	twisted pair cable	fiber optic cable	electrical cable	twisted pair cable
25	_________ cable consists of central conductor and sheild.	coaxial cable	twisted pair cable	fiber optic cable	electrical cable	coaxial cable
26	________ cable is used in backbone networks, cable Tv networks and fast ethernet networks	coaxial cable	twisted pair cable	fiber optic cable	electrical cable	fiber optic cable
27	________ are used for cellular phone, satellite and wireless LAN communications	Micro Waves	Infrared Waves	Sine Waves	Radio Waves	Micro Waves
28	Which of the following is used for short range communications?	Micro Waves	Infrared Waves	Sine Waves	Radio Waves	Infrared Waves
29	Three methods of switching are __________	circuit switching, packet switching, and protocol switching	circuit switching, packet switching, and message switching	Loop switching, packet switching, and message switching	Node switching, packet switching, and message switching	circuit switching, packet switching, and message switching
30	A switched network consists of a series of interlinked nodes, called __________	endpoints	packets	switches	links	switches
31	Switching in Internet is done by using datagram approach to packet switching at the __________	network layer	application layer	data link layer	physical layer	network layer
32	A Circuit-Switched Network is made of a set of switches connected by physical __________	media	links	nodes	lines	links
33	A switch in a datagram network uses a __________	destination address	sender address	routing table	header	routing table
34	Routing processor searching for routing table is called __________	switch fabric	buffer	table lookup	rolling table	table lookup
35	In ________ the resources need to be reserved during the setup phase.	circuit switching	packet switching	message switching	datagram switching	circuit switching
36	In Circuit Switching, resources needs to be reserved during the ________	data transfer phase	teardown phase.	setup phase	propagation phase	setup phase
37	In ________ there is no resource reservation, resources are alloted on demand	circuit switching	packet switching	message switching	datagram switching	packet switching
38	In a packet-switched network, resources are allocated _________	randomly	on demand	reserved already	automatically	on demand
39	Actual communication in a circuit-switched network requires __________	one phase	two phases	three phases	four phases	three phases

40	Setup, data transfer, and connection teardown are three phases of __________	circuit switching	packet switching	message switching	datagram switching	circuit switching
41	Circuit switching takes place at the __________	network layer	application layer	data link layer	physical layer	physical layer
42	A local telephone network is an example of a _______ ne	packet switched	circuit switched	message switched	virtual switched	packet switched
43	which of the following network requires that all channels in a message transmission path be of the same speed?	packet switched	circuit switched	message switched	virtual switched	circuit switched
44	Which of the networks allow different speed links?	packet switched	circuit switched	message switched	virtual switched	packet switched
45	Which of the networks allow pipelining effect?	packet switched	circuit switched	message switched	virtual switched	packet switched
46	HFC stands for __________	High Fiber cable	High Frequency Cable	Hybrid Fiber-Coaxial	Hybrid Frequency Cable	High Frequency Cable
47	Cable TV networks started to distribute broadcast video signals to locations in late __________	1940s	1950s	1960s	1970s	1940s
48	When Cable TV is used for data transfer then downstream band has __________	11 channels	22 channels	33channels	44 channels	33channels
49	DSL stands for ______	Digital Subscriber Line	Data Subscriber Line	Digital Switched Line	Data SwitchedLine	Digital Subscriber Line
50	Distance of Symmetric Digital Subscriber Line is ________	18000	12000	10000	30000	12000

Error Correction & Detection:

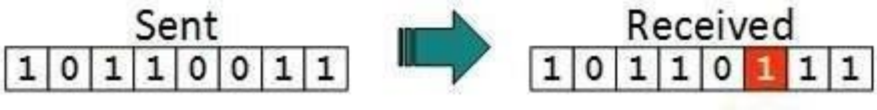
There are many reasons such as noise, cross-talk etc., which may help data to get corrupted during transmission. The upper layers work on some generalized view of network architecture and are not aware of actual hardware data processing. Hence, the upper layers expect error-free transmission between the systems. Most of the applications would not function expectedly if they receive erroneous data. Applications such as voice and video may not be that affected and with some errors they may still function well.

Data-link layer uses some error control mechanism to ensure that frames (data bit streams) are transmitted with certain level of accuracy. But to understand how errors is controlled, it is essential to know what types of errors may occur.

Types of Errors:

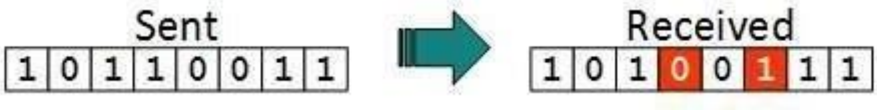
There may be three types of errors:

- **Single bit error**



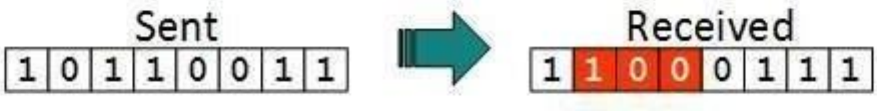
In a frame, there is only one bit, anywhere though, which is corrupt.

- **Multiple bits error**



Frame is received with more than one bits in corrupted state.

- **Burst error**



Frame contains more than1 consecutive bits corrupted.

Error control mechanism may involve two possible ways:

- Error detection
- Error correction

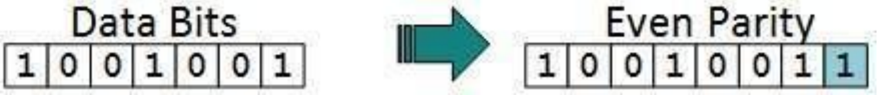
Error Detection:

Errors in the received frames are detected by means of Parity Check and Cyclic Redundancy Check (CRC). In both cases, few extra bits are sent along with actual data to confirm that bits received at other end are same as they were sent. If the counter-check at receiver' end fails, the bits are considered corrupted.

Parity Check

One extra bit is sent along with the original bits to make number of 1s either even in case of even parity, or odd in case of odd parity.

The sender while creating a frame counts the number of 1s in it. For example, if even parity is used and number of 1s is even then one bit with value 0 is added. This way number of 1s remains even.If the number of 1s is odd, to make it even a bit with value 1 is added.

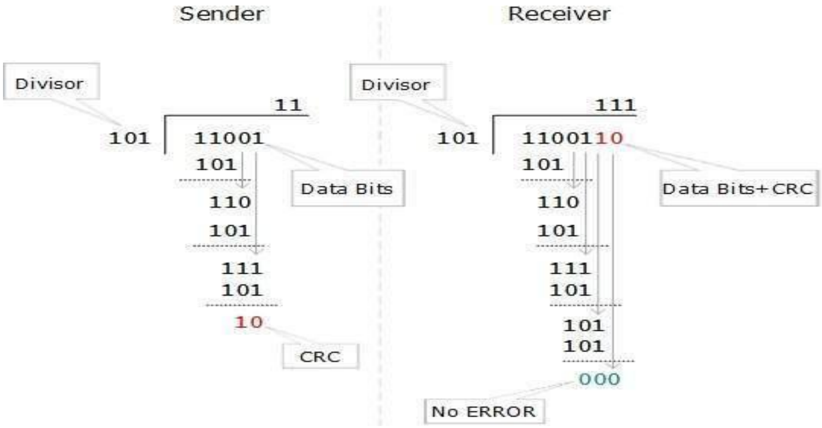


The receiver simply counts the number of 1s in a frame. If the count of 1s is even and even parity is used, the frame is considered to be not-corrupted and is accepted. If the count of 1s is odd and odd parity is used, the frame is still not corrupted.

If a single bit flips in transit, the receiver can detect it by counting the number of 1s. But when more than one bits are erro neous, then it is very hard for the receiver to detect the error.

Cyclic Redundancy Check (CRC)

CRC is a different approach to detect if the received frame contains valid data. This technique involves binary division of the data bits being sent. The divisor is generated using polynomials. The sender performs a division operation on the bits being sent and calculates the remainder. Before sending the actual bits, the sender adds the remainder at the end of the actual bits. Actual data bits plus the remainder is called a codeword. The sender transmits data bits as codewords.



At the other end, the receiver performs division operation on codewords using the same CRC divisor. If the remainder contains all zeros the data bits are accepted, otherwise it is considered as there some data corruption occurred in transit.

Error Correction:

In the digital world, error correction can be done in two ways:

- **Backward Error Correction** When the receiver detects an error in the data received, it requests back the sender to retransmit the data unit.
- **Forward Error Correction** When the receiver detects some error in the data received, it executes error-correcting code, which helps it to auto-recover and to correct some kinds of errors.

The first one, Backward Error Correction, is simple and can only be efficiently used where retransmitting is not expensive. For example, fiber optics. But in case of wireless transmission retransmitting may cost too much. In the latter case, Forward Error Correction is used.

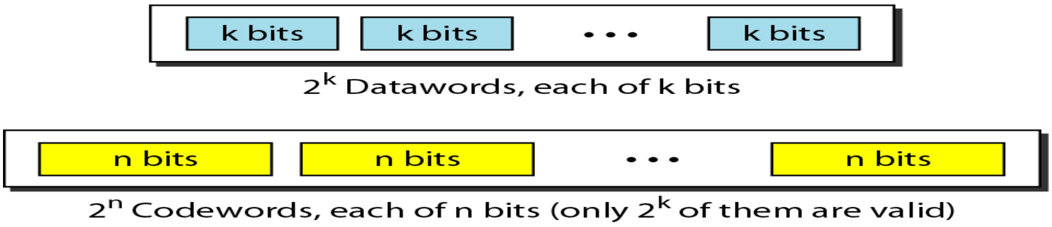
To correct the error in data frame, the receiver must know exactly which bit in the frame is corrupted. To locate the bit in error, redundant bits are used as parity bits for error detection. For example, we take ASCII words (7 bits data), then there could be 8 kind of information we need: first seven bits to tell us which bit is error and one more bit to tell that there is no error.

For m data bits, r redundant bits are used. r bits can provide 2r combinations of information. In m+r bit codeword, there is possibility that the r bits themselves may get corrupted. So the number of r bits used must inform about m+r bit locations plus no-error information, i.e. m+r+1.

BLOCK CODING:

In block coding, we divide our message into blocks, each of k bits, called datawords. We add r redundant bits to each block to make the length n = k + r. The resulting n-bit blocks are called codewords.

We have a set of datawords, each of size *k*, and a set of codewords, each of size of *n*. With *k* bits, we can create a combination of 2^k datawords; with *n* bits, we can create a combination of 2^n codewords. Since $n > k$, the number of possible codewords is larger than the number of possible datawords. The block coding process is one-to-one; the same dataword is always encoded as the same codeword. This means that we have $2^n - 2^k$ codewords that are not used. We call these codewords invalid or illegal. Figure below shows the situation.


k bits
k bits
• • •
k bits
2^k Datawords, each of k bits
n bits
n bits
• • •
n bits
2^n Codewords, each of n bits (only 2^k of them are valid)

Linear Block Codes:

In the linear block codes, the parity bits and message bits have a linear combination, which means that the resultant code word is the linear combination of any two code words.

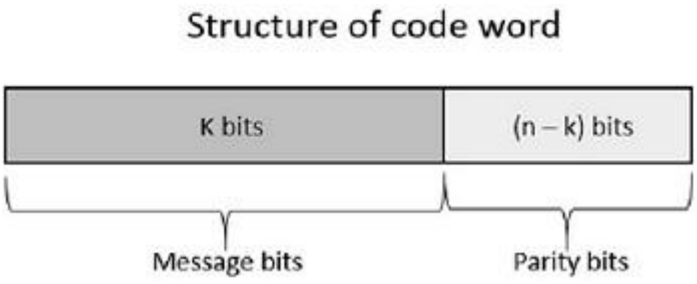
Let us consider some blocks of data, which contains **k** bits in each block. These bits are mapped with the blocks which has **n**bits in each block. Here **n** is greater than **k**. The transmitter adds redundant bits which are **(n-k)** bits. The ratio **k/n** is the **code rate**. It is denoted by **r** and the value of **r** is **r < 1**.

The **(n-k)** bits added here, are **parity bits**. Parity bits help in error detection and error correction, and also in locating the data. In the data being transmitted, the left most bits of the code word correspond to the message bits, and the right most bits of the code word correspond to the parity bits.

Systematic Code

Any linear block code can be a systematic code, until it is altered. Hence, an unaltered block code is called as a **systematic code**.

Following is the representation of the **structure of code word**, according to their allocation.



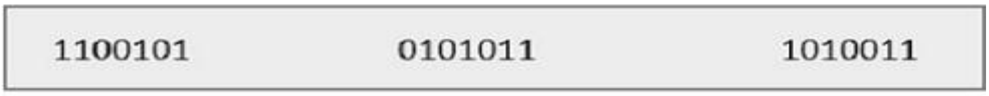
If the message is not altered, then it is called as systematic code. It means, the encryption of the data should not change the data.

Convolution Codes

So far, in the linear codes, we have discussed that systematic unaltered code is preferred. Here, the data of total **n** bits if transmitted, **k** bits are message bits and **(n-k)** bits are parity bits.

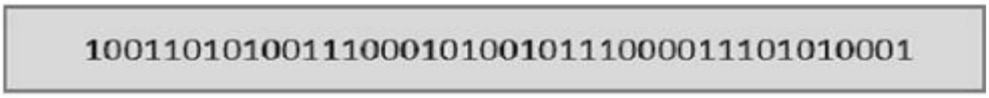
In the process of encoding, the parity bits are subtracted from the whole data and the message bits are encoded. Now, the parity bits are again added and the whole data is again encoded.

The following figure quotes an example for blocks of data and stream of data, used for transmission of information.



1100101 0101011 1010011

Example for blocks of data



100110101001110001010010111000011101010001

Example for stream of data

The whole process, stated above is tedious which has drawbacks. The allotment of buffer is a main problem here, when the system is busy.

This drawback is cleared in convolution codes. Where the whole stream of data is assigned symbols and then transmitted. As the data is a stream of bits, there is no need of buffer for storage.

Hamming Codes

The linearity property of the code word is that the sum of two code words is also a code word. Hamming codes are the type of **linear error correcting** codes, which can detect up to two bit errors or they can correct one bit errors without the detection of uncorrected errors.

While using the hamming codes, extra parity bits are used to identify a single bit error. To get from one-bit pattern to the other, few bits are to be changed in the data. Such number of bits can be termed as **Hamming distance**. If the parity has a distance of 2, one-bit flip can be detected. But this can't be corrected. Also, any two bit flips cannot be detected.

However, Hamming code is a better procedure than the previously discussed ones in error detection and correction.

BCHCodes

BCH codes are named after the inventors **B**ose, **C**haudari and **H**ocquenghem. During the BCH code design, there is control on the number of symbols to be corrected and hence multiple bit correction is possible. BCH codes is a powerful technique in error correcting codes.

For any positive integers $\mathbf{m \geq 3}$ and $\mathbf{t < 2^{m-1}}$ there exists a BCH binary code. Following are the parameters of such code.

Block length $\mathbf{n = 2^m - 1}$

Number of parity-check digits $\mathbf{n - k \leq mt}$

Minimum distance $\mathbf{d_{min} \geq 2t + 1}$

This code can be called as **t-error-correcting BCH code**.

Checksum

- In checksum error detection scheme, the data is divided into k segments each of m bits.
- In the sender’s end the segments are added using 1’s complement arithmetic to get the sum. The sum is complemented to get the checksum.
- The checksum segment is sent along with the data segments.
- At the receiver’s end, all received segments are added using 1’s complement arithmetic to get the sum. The sum is complemented.
- If the result is zero, the received data is accepted; otherwise discarded.

Cyclic codes:

Cyclic codes are used for error correction. They are mainly used to correct double errors and burst errors.

Hence, these are a few error correcting codes, which are to be detected at the receiver. These codes prevent the errors from getting introduced and disturb the communication. They also prevent the signal from getting tapped by unwanted receivers.

A CRC will be valid if and only if it satisfies the following requirements:

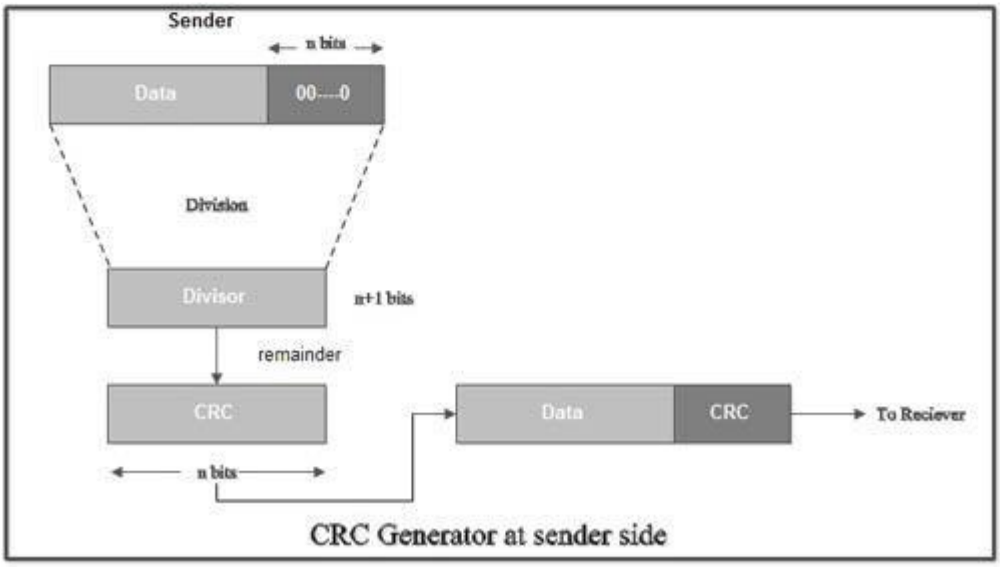
1. It should have exactly one less bit than divisor.

2. Appending the CRC to the end of the data unit should result in the bit sequence which is exactly divisible by the divisor.

• The various steps followed in the CRC method are

1. A string of n as is appended to the data unit. The length of predetermined divisor is n+ 1.

2. The newly formed data unit *i.e.* original data + string of n as are divided by the divisor using binary division and remainder is obtained. This remainder is called CRC.



CRC Generator at sender side

3. Now, string of n Os appended to data unit is replaced by the CRC remainder (which is also of n bit).

4. The data unit + CRC is then transmitted to receiver.

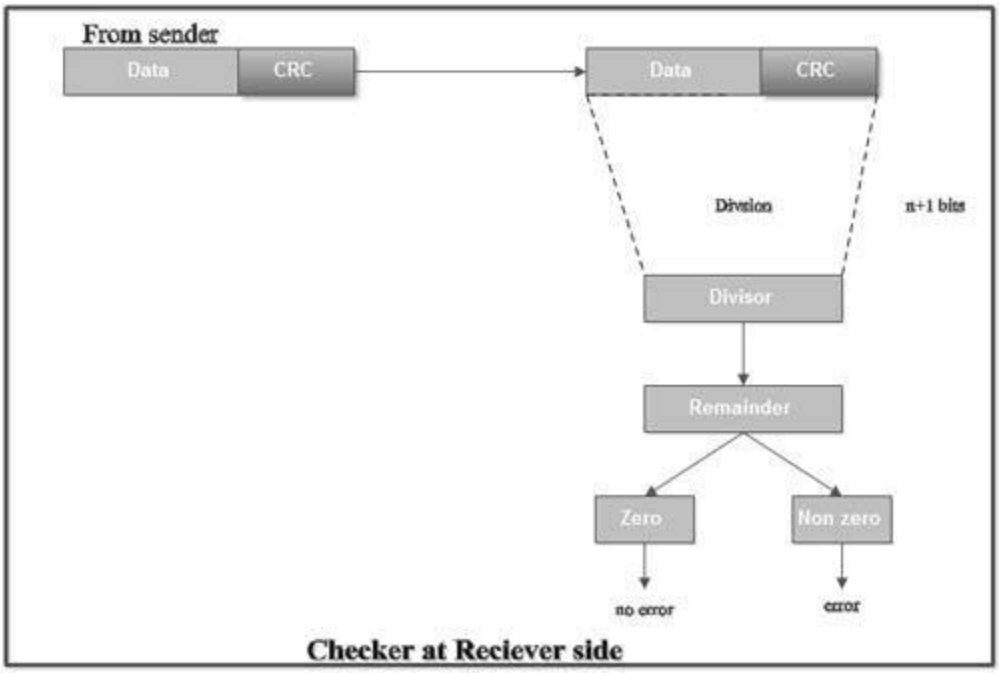
5. The receiver on receiving it divides data unit + CRC by the same divisor & checks the remainder.

6. If the remainder of division is zero, receiver assumes that there is no error in data and it accepts it.

7. If remainder is non-zero then there is an error in data and receiver rejects it.

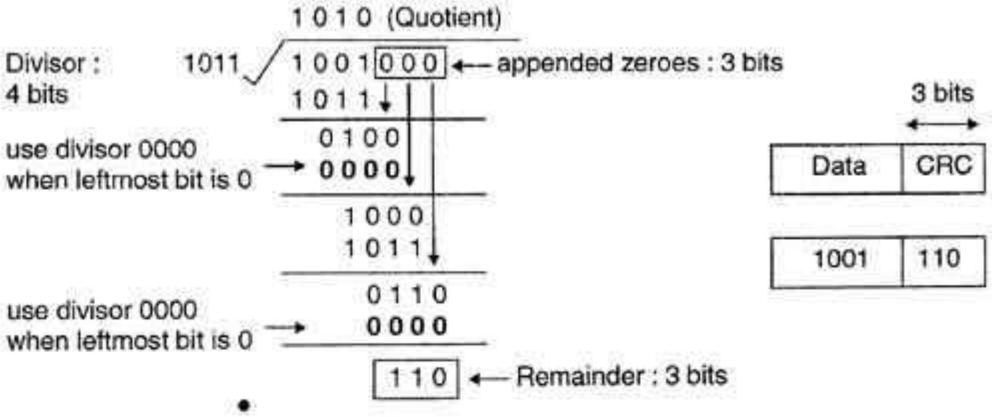
• For example, if data to be transmitted is 1001 and predetermined divisor is 1011. The procedure given below is used:

1. String of 3 zeroes is appended to 1011 as divisor is of 4 bits. Now newly formed data is 1011000.



Checker at Reciever side

1. Data unit 1011000 is divided by 1011.



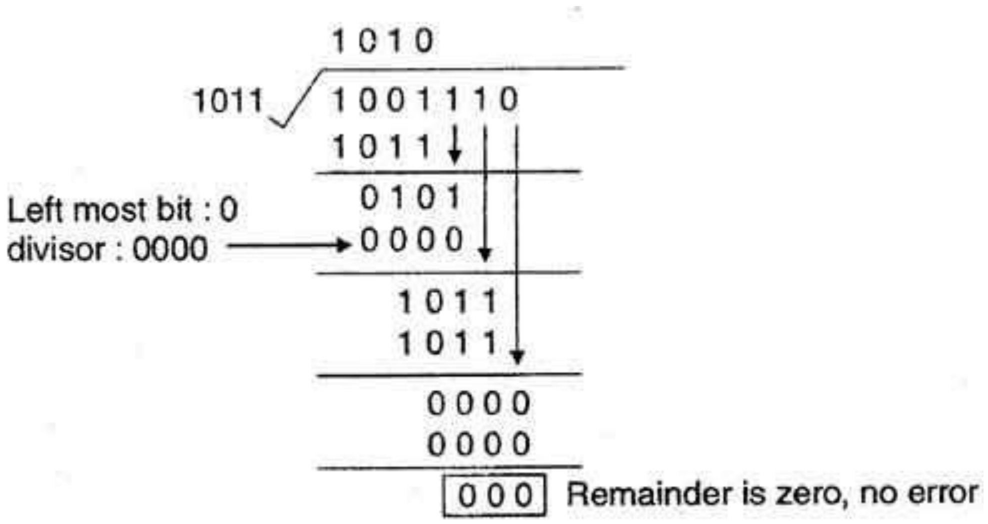
CRC generated (Binary division)

2. During this process of division, whenever the leftmost bit of dividend or remainder is 0, we use a string of Os of same length as divisor. Thus in this case divisor 1011 is replaced by 0000.

3. At the receiver side, data received is 1001110.

4. This data is again divided by a divisor 1011.

5. The remainder obtained is 000; it means there is no error.



CRC decoded (binary division)

- CRC can detect all the burst errors that affect an odd number of bits.
- The probability of error detection and the types of detectable errors depends on the choice of divisor.

Framing:

A point-to-point connection between two computers or devices consists of a wire in which data is transmitted as a stream of bits. However, these bits must be *framed* into discernible blocks of information. Framing is a function of the data link layer. It provides a way for a sender to transmit a set of bits that are meaningful to the receiver. Ethernet, token ring, frame relay, and other data link layer technologies have their own frame structures. Frames have headers that contain information such as error-checking codes.

There are three different types of framing, each of which provides a way for the sender to tell the receiver where the block of data begins and ends:

- **Byte-oriented framing** Computer data is normally stored as alphanumeric characters that are encoded with a combination of 8 bits (1 byte). This type of framing differentiates one byte from another. It is an older style of framing that was used in the terminal/mainframe environment. Examples of byte-oriented framing include IBM's BISYNC protocol.
- **Bit-oriented framing** :

  This type of framing allows the sender to transmit a long string of bits at one time. IBM's SDLC (Synchronous Data Link Control) and HDLC (High-level Data Link Control) are examples of bit-oriented protocols. Most LANs use bit-oriented framing. There is usually a maximum frame size. For example, Ethernet has a maximum frame size of 1,526 bytes. The beginning and end of a frame is signaled with a special bit sequence (01111110 for HDLC). If no data is being transmitted, this same sequence is continuously transmitted so the end systems remain synchronized.

- **Clock-based framing** In a clock-based system, a series of repetitive pulses are used to maintain a constant bit rate and keep the digital bits aligned in the data stream. SONET (Synchronous Optical Network) is a synchronous system in which all the clocks in the network are synchronized back to a master clock reference. SONET frames are then positioned within the clocked stream.

The advantage of using frames is that data is broken up into recoverable chunks that can easily be checked for corruption. A glitch in the line during the transmission will corrupt some frames. Only the lost frames and not the entire set of data needs to be retransmitted.

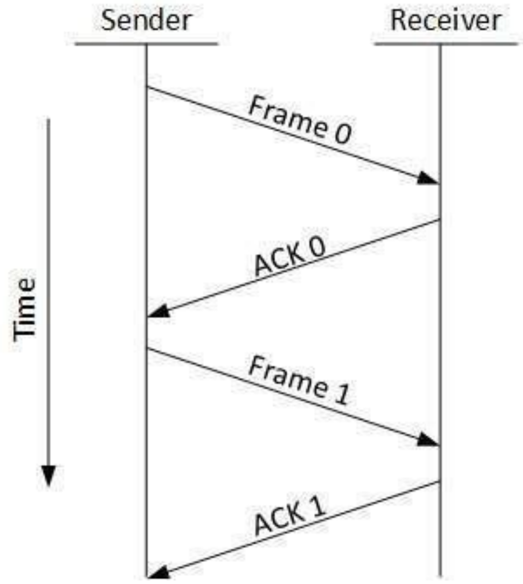
Flow Control:

When a data frame (Layer-2 data) is sent from one host to another over a single medium, it is required that the sender and receiver should work at the same speed. That is, sender sends at a speed on which the receiver can process and accept the data. What if the speed (hardware/software) of the sender or receiver differs? If sender is sending too fast the receiver may be overloaded, (swamped) and data may be lost.

Two types of mechanisms can be deployed to control the flow:

- **Stop and Wait**

This flow control mechanism forces the sender after transmitting a data frame to stop and wait until the acknowledgement of the data-frame sent is received.



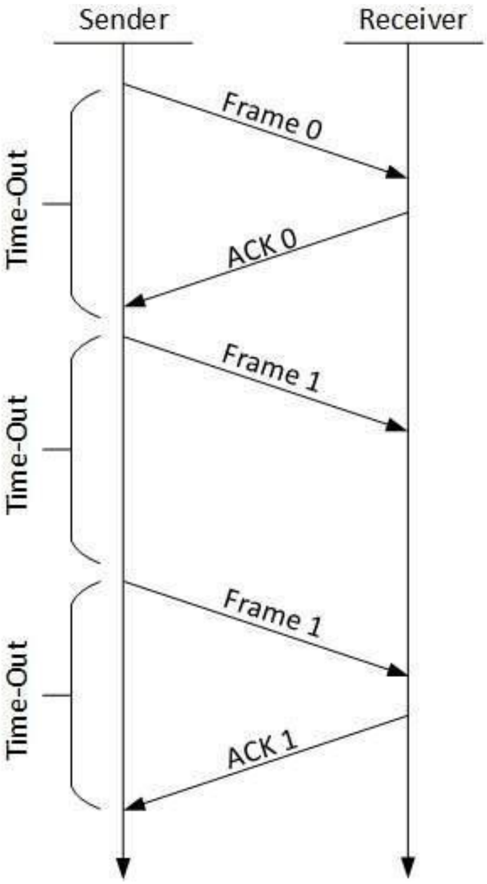
- **Sliding Window**

  In this flow control mechanism, both sender and receiver agree on the number of data-frames after which the acknowledgement should be sent. As we learnt, stop and wait flow control mechanism wastes resources, this protocol tries to make use of underlying resources as much as possible.

Stop-and-Wait ARQ:

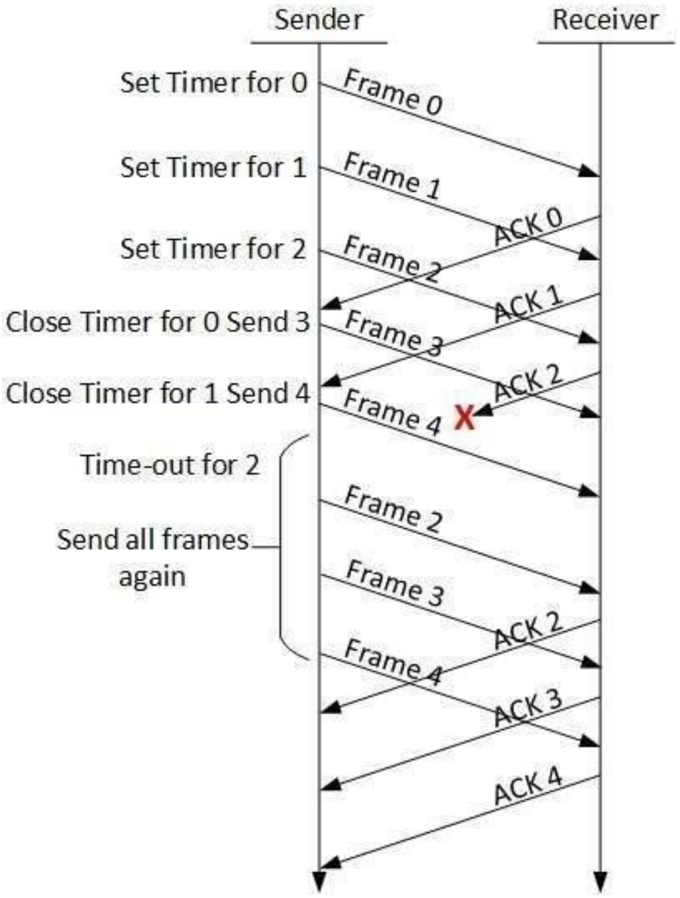
The following transition may occur in Stop-and-Wait ARQ:

- The sender maintains a timeout counter.
- When a frame is sent, the sender starts the timeout counter.
- If acknowledgement of frame comes in time, the sender transmits the next frame in queue.
- If acknowledgement does not come in time, the sender assumes that either the frame or its acknowledgement is lost in transit. Sender retransmits the frame and starts the timeout counter.
- If a negative acknowledgement is received, the sender retransmits the frame.



Go-Back-N ARQ:

Stop and wait ARQ mechanism does not utilize the resources at their best. When the acknowledgment is received, the sender sits idle and does nothing. In Go-Back-N ARQ method, both sender and receiver maintain a window.



The sending-window size enables the sender to send multiple frames without receiving the acknowledgement of the previous ones. The receiving-window enables the receiver to receive multiple frames and acknowledge them. The receiver keeps track of incoming frame's sequence number.

When the sender sends all the frames in window, it checks up to what sequence number it has received positive acknowledgement. If all frames are positively acknowledged, the sender sends next set of frames. If sender finds that it has received NACK or has not receive any ACK for a particular frame, it retransmits all the frames after which it does not receive any positive ACK.

Point-to-Point Protocol (PPP):

PPP was devised by IETF (Internet Engineering Task Force) to create a data link protocol for point to point lines that can solve all the problems present in SLIP.

PPP is most commonly used data link protocol. It is used to connect the Home PC to the server of ISP via a modem.

This protocol offers several facilities that were not present in SLIP. Some of these facilities are:

1. PPP defines the format of the frame to be exchanged between the devices.

2. It defines link control protocol (LCP) for:-

   (a) Establishing the link between two devices.
   (b) Maintaining this established link.
   (c) Configuring this link.
   (d) Terminating this link after the transfer.

3. It defines how network layer data are encapsulated in data link frame.

4. PPP provides error detection.

5. Unlike SLIP that supports only IP, PPP supports multiple protocols.

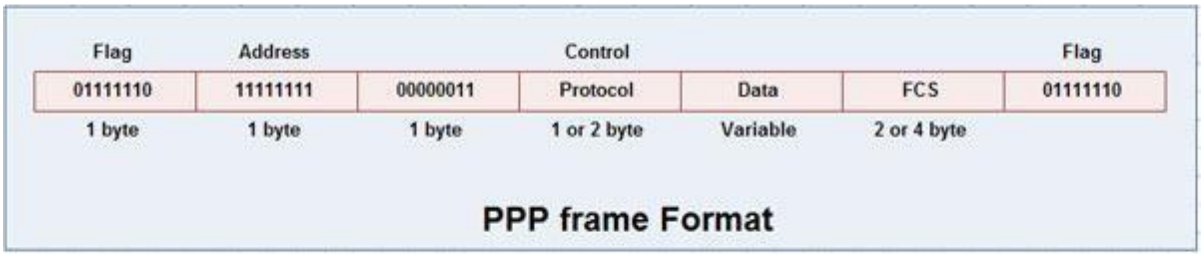
6. PPP allows the IP address to be assigned at the connection time i.e. dynamically. Thus a temporary IP address can be assigned to each host.

7. PPP provides multiple network layer services supporting a variety of network layer protocol. For this PPP uses a protocol called NCP (Network Control Protocol).

8. It also defines how two devices can authenticate each other.

PPP Frame Format

The frame format of PPP resembles HDLC frame. Its various fields are:



Flag	Address		Control			Flag
01111110	11111111	00000011	Protocol	Data	FCS	01111110
1 byte	1 byte	1 byte	1 or 2 byte	Variable	2 or 4 byte	

PPP frame Format

1. Flag field: Flag field marks the beginning and end of the PPP frame. Flag byte is 01111110. (1 byte).

2. Address field: This field is of 1 byte and is always 11111111. This address is the broadcast address i.e. all the stations accept this frame.

3. Control field: This field is also of 1 byte. This field uses the format of the U-frame (unnumbered) in HDLC. The value is always 00000011 to show that the frame does not contain any sequence numbers and there is no flow control or error control.

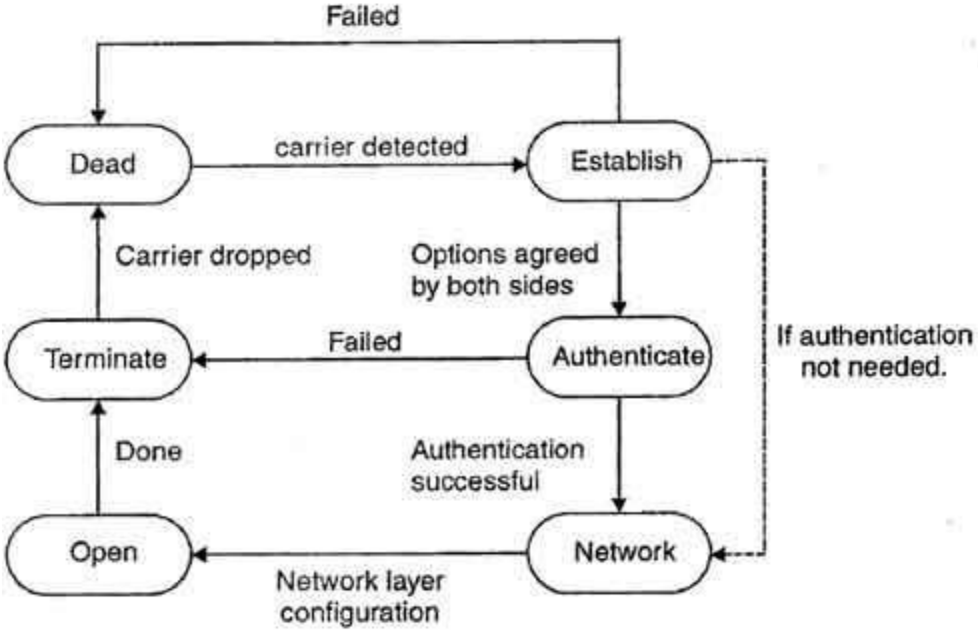
4. Protocol field: This field specifies the kind of packet in the data field i.e. what is being carried in data field.

5. Data field: Its length is variable. If the length is not negotiated using LCP during line set up, a default length of 1500 bytes is used. It carries user data or other information.

6. FCS field: The frame checks sequence. It is either of 2 bytes or 4 bytes. It contains the checksum.

Transition Phases in PPP

The PPP connection goes through different states as shown in fig.


Failed
Dead
carrier detected
Establish
Carrier dropped
Options agreed by both sides
Terminate
Failed
Authenticate
If authentication not needed.
Done
Authentication successful
Open
Network
Network layer configuration

Transition phases

1. Dead: In dead phase the link is not used. There is no active carrier and the line is quiet.

2. Establish: Connection goes into this phase when one of the nodes start communication. In this phase, two parties negotiate the options. If negotiation is successful, the system goes into authentication phase or directly to networking phase. LCP packets are used for this purpose.

3. Authenticate: This phase is optional. The two nodes may decide during the establishment phase, not to skip this phase. However if they decide to proceed with authentication, they send several authentication packets. If the result is successful, the connection goes to the networking phase; otherwise, it goes to the termination phase.

4. Network: In network phase, negotiation for the network layer protocols takes place. PPP specifies that two nodes establish a network layer agreement before data at the network layer can be exchanged. This is because PPP supports several protocols at network layer. If a node is running multiple protocols simultaneously at the network layer, the receiving node needs to know which protocol will receive the data.

5. Open: In this phase, data transfer takes place. The connection remains in this phase until one of the endpoints wants to end the connection.

6. Terminate: In this phase connection is terminated.

KarpagamAcademy of Higher Education

(Established Under Section 3 of UGC Act 1956) Eachanari Post,
Coimbatore – 641 021. INDIA
Phone : 0422-2611146, 2611082 Fax No : 0422 -2611043

Enable | Enlighten | Enrich
(Deemed to be University)
(Under Section 3 of UGC Act 1956)

DEPARTMENT OF COMPUTER APPLICATIONS

BCA (2017-2020 BATCH)

COURSE NAME: COMPUTER NETWORKS COURSE CODE: 17CAU303

UNIT III - POSSIBLE QUESTIONS

PART – A (20 Marks)

(Q.No 1 to 20 Online Examinations)

PART – B

(Each question carries two marks)

1. What are the responsibilities of data link layer?
2. What are the types of errors?
3. Define ARQ
4. What is hamming distance?
5. Define Check sum.
6. Define CRC.
7. What is framing?
8. What are the three kinds of framing?
9. Define flow control.
10. Define PPP.

PART –C

(Each question carries six marks)

1. Write about block coding and explain how the errors are detected and corrected using block coding?
2. Explain the framing in data link layer.
3. Explain Cyclic Redundancy Check (CRC) code?
4. Error detection and error correction in data link layer.
5. Explain Stop and wait ARQ protocol with a neat diagram.
6. Explain the point to point protocol on Internet

7.Explain how the errors are detected and corrected using Checksum.

8. Describe about the Selective Repeat ARQ protocol used in noisy channels.
9. Describe the protocols used in noiseless channels with a neat diagram.
10. Discuss in detail about the point to point protocol.

Karpagam Academy of Higher Education

Department of Computer Applications

BCA (2017-2020 Batch)

COMPUTER NETWORKS (17CAU303)

UNIT- III

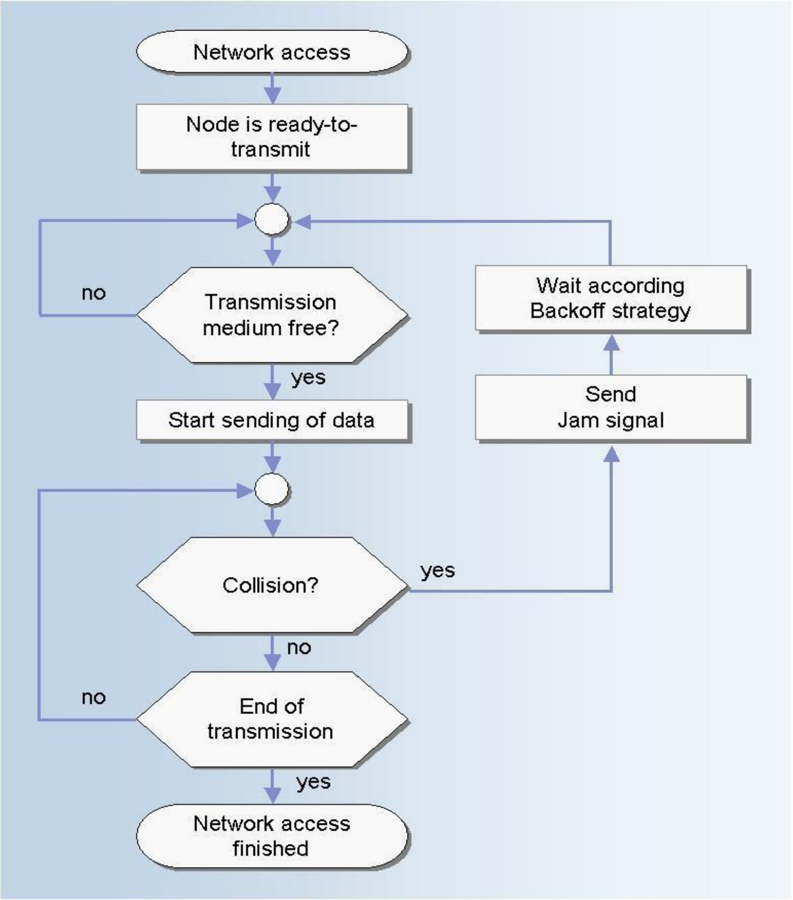
S.No	Question	Option1	Option2	Option3	Option4	Answer
1	Transmission errors are usually detected at the _______ layer of OSI model	physical	datalink	network	transport	physical
2	Datalink layer imposes a________ mechanism to avoid overwhelming the receiver	flow control	error control	access control	file transfer	flow control
3	Error control mechanism of datalink layer is achieved through a added to the end of frame.	header	trailer	address	frames	trailer
4	The datalink layer is responsible for moving _____ from one hop to next	packets	frames	signals	message	frames
5	In a single bit error,how many bits in the data unit are changed?	one	two	four	five	one
6	In a _______ error, only one bit in the data unit are changed.	single-bit	multi-bit	burst	syntax	single-bit
7	In a burst error,how many bits in a data unit are changed?	less than 2	2 or more than 2	2	3	2 or more than 2
8	In a _______ error means that 2 or more bits in the data unit have changed.	single-bit	multi-bit	burst	syntax	burst
9	The length of the burst error is measured from _______	first bit to last bit	first corrupted bit to last corrupted bit	two	three	first corrupted bit to last corrupted bit
10	Single bit error will least occur in ______ data transmissions	serial	parallel	synchronous	asynchronous	serial
11	To detect errors or correct errors,we need to send with data.	address	frames	redundant bits	packets	redundant bits
12	_________ is used to see if any error has occurred in the message.	error correction	error detection	retransmission	translation	error detection
13	_________ is used to know the exact number of bits that are corrupted and their location in tne message.	error correction	error detection	retransmission	translation	error correction
14	In block coding,we divide our message intp blocks,each of k bits.called	dataword	codeword	message	segment	dataword
15	In block coding,the length of the block is ______	k	r	k+r	k-r	k+r
16	Block coding can detect only _______error	single	burst	multiple	multilevel	single
17	We need _______ redundant bits for error correction than for error detection	less	more	equal	less than or equal to	more
18	The corresponding codeword for the dataword 01 is	011	000	101	110	011
19	Coding schemes are divided into ______ broad categories	2	3	4	5	2
20	Hamming distance between two eords x and y is represented as	f(x,y)	d(x,y)	h(x,y)	e(x,y)	d(x,y)
21	The hamming distance can easily be found if we apply the operation	XOR	OR	AND	NAND	XOR
22	The ______ hamming distance is the smallest hamming distance between all possible pairs in a set of words	minimum	maximum	equal	not equal	minimum
23	The hamming distance d(000,011) is _____	1	0	2	3	2
24	To guarantee correction of upto t errors in all cases,the minimum hamming distance in a block code must be	d(min)=2t+1	d(min)=2t-1	d(min)=2t	d(min)=t+1	d(min)=2t+1
25	To guarantee correction of upto s errors in all cases,the minimum hamming distance in a block code must be	d(min)=s-1	d(min)=s+1	d(min)=t-1	d(min)=t+1	d(min)=s+1
26	A simple_parity check code is a single bit error detecting code in which n= with d(min)=2	K	K*1	K-1	K+1	K+1
27	The codeword corresponding to the dataword 1111 is	11110	11111	11101	11011	11110
28	A simple_parity check code can detect an _______ Number of errors	odd	even	prime	natural	odd
29	The hamming code is a method of _________	error detection	error correction	retransmission	translation	error correction
30	To make the hamming code respond to a burst error of size N we neeed to make codewords of our frame	N+1	N-1	N	0	N
31	CRC stands for______	Cyclic Redundancy Check	Cyclic Redundancy Count	Cyclic Redundancy Code	Cyclic Redundancy Correction	Cyclic Redundancy Check
32	CRC is used in network such as _____	WAN	LAN and WAN	LAN	MAN	LAN and WAN
33	In CRC there is no error if the remainder at the receiver is	equal to the remainder at the sender	zero	non zero	equal to the quotient at the sender	Zero
34	At the CRC checker _____ means that the data unit is damaged.	string of 0's	string of 1's	a string of alternating 1's and 0's	a non-zero remainder	a non-zero remainder
35	______is a regulation of data transmission so that the receiver buffer do not become overwhelmed	flow control	error control	access control	none of the above	flow control
36	________ in the datalink layer separates a message from one source ti a destination or from other message to	packets	address	framing	none of the above	framing
37	_______ is the process of adding 1 extra byte whenever there is a flag or escape character in text	byte stuffing	redundancy	bit_stuffing	none of the above	byte stuffing
38	______ is the process of adding 1 extra 0 whenever five consecutive 1's follows a 0 in the data.	byte stuffing	redundancy	bit_stuffing	none of the above	bit_stuffing
39	_______ in the data link layer is based on automatic repeat request,which is the retransmission of data	error control	flow control	access control	framing	error control
40	At any time an error is detected in an exchange specified frames are retransmitted and process is called	ARQ	ACK	NAK	SEL	ARQ
41	The datalink layer at the sender side gets data from its layer	network	physical	application	transport	network
42	ARQ stands for ______	acknowledge repeat request	automatic repeat request	automatic repeat quantisation	automatic retransmission request	automatic repeat request
43	Which of the following is not a data link layer function?	framing	error control	flow control	routing	routing
44	In stop and wait ARQ ,the sequence of numbers is based on	modulo-2-arithmetic	modulo-12-arithmetic	modulo-N-arithmetic	other modulo-arithmetic	modulo-2-arithmetic
45	Error correction in _______is done by keeping a copy of the send frames and retransmitting of the frame when	stop and wait ARQ	ARQ	ACK	NAQ	stop and wait ARQ
46	In the Go_Back N protocol,the sequence numbers are modulo	2^{m}	2^{m-1}	2^{m+1}	2	2^{m}
47	Piggypacking is used to improve the efficiency of the protocols.	bidirectional	unidirectional	multidirectional	reversedirectional	bidirectional
48	The send window can slide _______slots when a valid acknowledgment arrive	one or more	one	two	two or more	one or more
49	The upper sublayer that is responsible for flow and error control is called control	logical	media access	A and B	all the above	logical
50	MAC stands for______	Media Address Control	Media Access Control	Medium Address Control	Medium Access Control	Media Access Control
51	The MAC sublayer co-ordinates the datalink task within a specified	LAN	MAN	WAN	LAN and MAN	LAN
52	The lower sublayer that is responsible for multiple access resolution is called control	Logical	media access	A and B	all the above	media access
53	In the sliding window method or flow control several frame can be at a time	transit	received	created	deleted	transit
54	The sliding window of the sender expands to the when acknowledgement are received	left	middle	right	center	right
55	Datalink layer divided into _______ functionality oriented sublayer.	2	3	4	5	2
56	The send window in Go_Back N maximum size can be	2^{m}	2^{m+1}	2	2^{m-1}	2m-1
57	In stop and wait ARQ and Go_Back_N ARQ,the size of the send window is	1	2	3	4	1
58	The relationship between m and n in hamming code is	n=2m-1	n=m	n=m-1	n=2m+1	n=2m-1
59	_______mechanism of datalink layer is achieved through added to the trailer added to the end of frame.	ARQ	ARC	Error control	Flow control	Error control
60	The _______layer at the sender site gets data from its network layer.	physical	datalink	application	transport	datalink

Multiple Access Protocol and Networks:

Carrier Sense Multiple Access/Collision Detection (CSMA/CD):

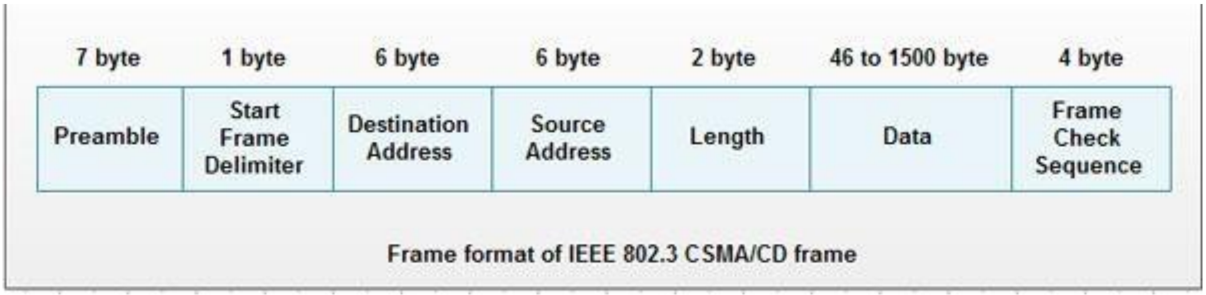
- **CS** means that stations first sense a carrier present on the media before transmitting their own signals.
- **MA** means that multiple stations can access the network media.
- **CD** means that if a collision is detected because of multiple simultaneous transmissions of signals, the stations that are transmitting signals stop, and then retransmit a short time later.
- Carrier Sense Multiple Access/Collision Detection, CSMA/CD is a Media Access Control (MAC) protocol.
- It defines how network devices respond when two devices attempt to use a data channel simultaneously and encounter a data collision.
- A type of media access control method for placing signals on baseband transmission networks.
- Baseband networks can carry only one data signal at a time, there must be some way of controlling which station has access to the media at any given time.
- In networking technologies that use CSMA/CD as their access method, a station first “listens” to the network media to make sure there is no signal already present from another station before it tries to place its own signal on the media.
- If a carrier signal is detected on the media, which indicates that a station is currently transmitting a signal, no other station can initiate a transmission until the carrier stops.
- If no carrier is detected, any station can transmit a signal.
- If two stations listen to the wire and detect no carrier signal, they may both decide to send signals simultaneously.
- If this happens, a collision occurs between the two signals generated. Next, both stations detect the collision and stop transmitting their signals immediately, sending out a jamming signal that informs all other stations on the network that a collision has occurred and that they should not transmit.

- Meanwhile, the two stations whose signals created the collision stop transmitting and wait random intervals of time (usually a few milliseconds) before attempting to retransmit.
- CSMA/CD is known as a contention method because computers contend for the chance to transmit data onto the network media. CSMA/CD is the standard access method for Ethernet networks.



Frame format of CSMA/CD

The frame format specified by IEEE 802.3 standard contains following fields.



7 byte	1 byte	6 byte	6 byte	2 byte	46 to 1500 byte	4 byte
Preamble	Start Frame Delimiter	Destination Address	Source Address	Length	Data	Frame Check Sequence

Frame format of IEEE 802.3 CSMA/CD frame

1. **Preamble**: It is seven bytes (56 bits) that provides bit synchronization. It consists of alternating Os and 1s. The purpose is to provide alert and timing pulse.

2. **Start Frame Delimiter (SFD)**: It is one byte field with unique pattern: 10 10 1011. It marks the beginning of frame.

3. **Destination Address (DA)**: It is six byte field that contains physical address of packet's destination.

4. **Source Address (SA)**: It is also a six byte field and contains the physical address of source or last device to forward the packet (most recent router to receiver).

5. **Length**: This two byte field specifies the length or number of bytes in data field.

6. **Data**: It can be of 46 to 1500 bytes, depending upon the type of frame and the length of the information field.

7. **Frame Check Sequence (FCS)**: This four byte field contains CRC for error detection.

There are several CSMA access modes:

- 1-persistent CSMA (IEEE 802.3)
  - If medium idle, transmit; if medium busy, wait until idle; then transmit with p=1.
  - If collision, waits random period and starts again.
- Non-persistent CSMA: if medium idle, transmit; otherwise wait a random time before re-trying.
  - Thus, station does not continuously sense channel when it is in use.
- P-persistent: when channel idle detected, transmits packet in the first slot with p.
- O-persistent CSMA:
  - This mode assigns a transmission order to each data node.

- When the medium becomes idle, the data node next in line can transmit data.
- The data node next in line waits for the medium to be idle again and then transmits its data.
- After each data node transmits data, the transmission order is updated to reflect what data nodes have already transmitted, moving each data node through the queue.

Ethernet LANs:

Ethernet is the name of the most commonly used LAN today. A LAN (Local Area Network) is a network of computers that covers a small area like a room, an office, a building or a campus. It is used in contrast with WAN (wide area network) which spans for much larger geographical areas. Ethernet is a network protocol that controls how data is transmitted over a LAN. Technically it is referred to as the IEEE 802.3 protocol.

The protocol has evolved and improved over time and can now deliver at the speed of a gigabit per second. That's one million kbps.

Many people have for their whole lives been using Ethernet without actually knowing it. It is most likely that the wired network in your office, at the bank and even at home is an Ethernet LAN. Besides, most desktop and laptop computers come with integrated an Ethernet card inside so that it is ready to be connected to an Ethernet LAN.

Requirements for Ethernet LAN:

To set up a small or big Ethernet LAN, you need the following:

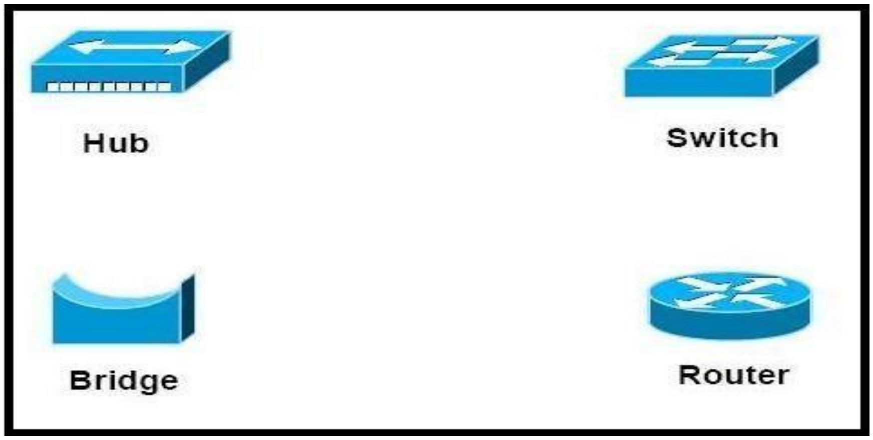
- Computers and devices to connect. An Ethernet connects any type of computer to its network as long as the device has an Ethernet adapter or network card.
- Network interface cards in the devices. This is either integrated into the motherboard of the computer or installed separately in the device. You also have USB versions of Ethernet cards like external dongles. An Ethernet card is simply known as a network card. It has ports (sort of a socket to which we can connect cables) that can accommodate cables for connection. There are normally two ports, one for an RJ-45 jack (see picture), that connect UTP cables, and one for a coaxial jack.

- A hub or gateway to connect your devices in a star network. A hub is a device that acts as a connecting point between devices on a network. It consists of several RJ-45 ports to which you plug the cables.
- Cables. UTP (unshielded twisted pair) cables are more commonly used in Ethernet LANs. This is the same type of cable used for landline telephone sets, but fatter, with 8 twisted pairs of wires of different colors inside. The end is crimped with an RJ-45 jack, which is a larger version of the (RJ-11) jacks that plug into your landline phone. When the Ethernet spans beyond a room to distances that reach hundreds or meters, coaxial cable is used. This is the same cable we use for TV, with a round single-core jack.
- Software to manage the network. Modern operating systems like recent versions of Windows, Linux and Mac OS are more than sufficient to manage Ethernet LANs. You just need the skills to do it. There is also third-party software that gives more feature and better control.

Working of Ethernet:

When a machine on the network wants to send data to another, it senses the carrier (which is the main wire connecting all the devices). If it is free, i.e. no one is sending anything, it sends the data packet on the network, and all other devices check the packet to see whether they are the recipient. The recipient consumes the packet. If there is already a packet on the highway, the device that wants to send holds back for some thousandths of a second to try again until it can send.

Connecting LAN and Back-Bone Networks:



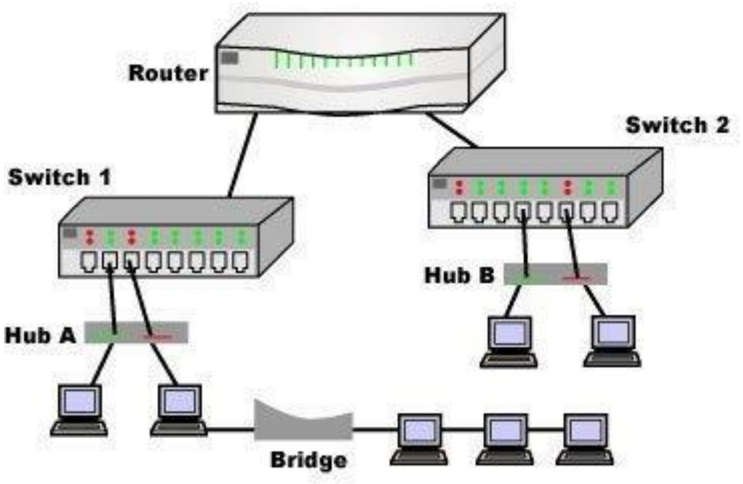
1. Repeater – A repeater operates at the physical layer. Its job is to regenerate the signal over the same network before the signal becomes too weak or corrupted so as to extend the length to which the signal can be transmitted over the same network. An important point to be noted about repeaters is that they do no amplify the signal. When the signal becomes weak, they copy the signal bit by bit and regenerate it at the original strength. It is a 2 port device.

2. Hub – A hub is basically a multiport repeater. A hub connects multiple wires coming from different branches, for example, the connector in star topology which connects different stations. Hubs cannot filter data, so data packets are sent to all connected devices. In other words, of all hosts connected through Hub remains one. Also, they do not have intelligence to find out best path for data packets which leads to inefficiencies and wastage.

3. Bridge – A bridge operates at data link layer. A bridge is a repeater, with add on functionality of filtering content by reading the MAC addresses of source and destination. It is also used for interconnecting two LANs working on the same protocol. It has a single input and single output port, thus making it a 2 port device.

4. Switch – A switch is a multi port bridge with a buffer and a design that can boost its efficiency (large number of ports imply less traffic) and performance. Switch is data link layer device. Switch can perform error checking before forwarding data, that makes it very efficient as it does not forward packets that have errors and forward good packets selectively to correct port only. In other words, switch divides collision domain of hosts, but broadcast remains same.

5. Routers – A router is a device like a switch that routes data packets based on their IP addresses. Router is mainly a Network Layer device. Routers normally connect LANs and WANs together and have a dynamically updating routing table based on which they make decisions on routing the data packets. Router divide broadcast domains of hosts connected through it.



6. Gateway – A gateway, as the name suggests, is a passage to connect two networks together that may work upon different networking models. They basically works as the messenger agents that take data from one system, interpret it, and transfer it to another system. Gateways are also called protocol converters and can operate at any network layer. Gateways are generally more complex than switch or router.

Network Layer Functions and Protocols:

Routing:

When a device has multiple paths to reach a destination, it always selects one path by preferring it over others. This selection process is termed as Routing. Routing is done by special network devices called routers or it can be done by means of software processes. The software based routers have limited functionality and limited scope.

A router is always configured with some default route. A default route tells the router where to forward a packet if there is no route found for specific destination. In case there are multiple path existing to reach the same destination, router can make decision based on the following information:

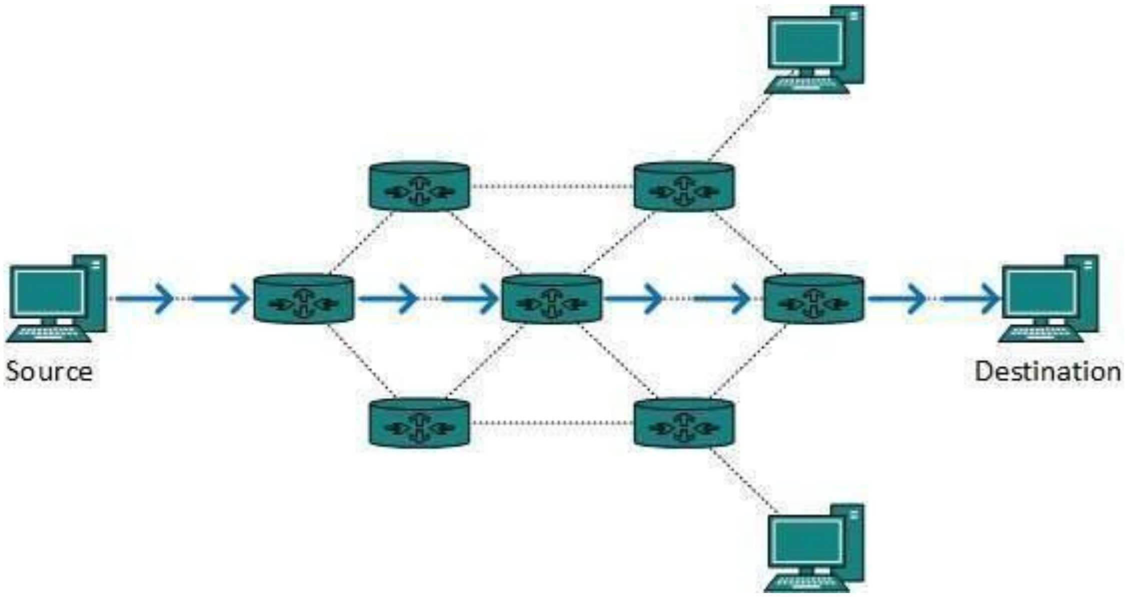
- Hop Count
- Bandwidth
- Metric
- Prefix-length
- Delay

Routes can be statically configured or dynamically learnt. One route can be configured to be preferred over others.

Routing Algorithm:

Unicast Routing:

Most of the traffic on the internet and intranets known as unicast data or unicast traffic is sent with specified destination. Routing unicast data over the internet is called unicast routing. It is the simplest form of routing because the destination is already known. Hence the router just has to look up the routing table and forward the packet to next hop.

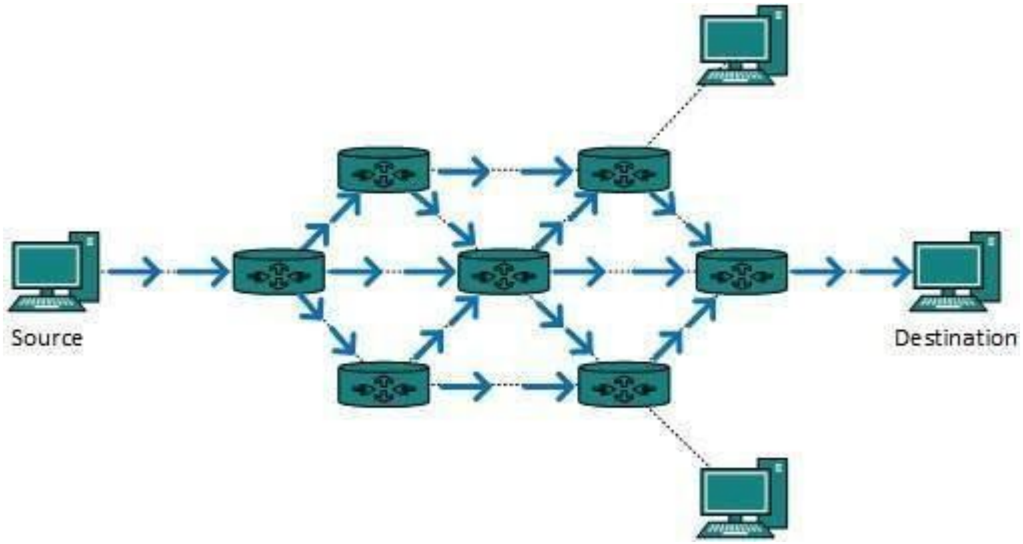


Broadcast Routing:

By default, the broadcast packets are not routed and forwarded by the routers on any network. Routers create broadcast domains. But it can be configured to forward broadcasts in some special cases. A broadcast message is destined to all network devices.

Broadcast routing can be done in two ways (algorithm):

- A router creates a data packet and then sends it to each host one by one. In this case, the router creates multiple copies of single data packet with different destination addresses. All packets are sent as unicast but because they are sent to all, it simulates as if router is broadcasting.
- This method consumes lots of bandwidth and router must destination address of each node.
- Secondly, when router receives a packet that is to be broadcasted, it simply floods those packets out of all interfaces. All routers are configured in the same way.

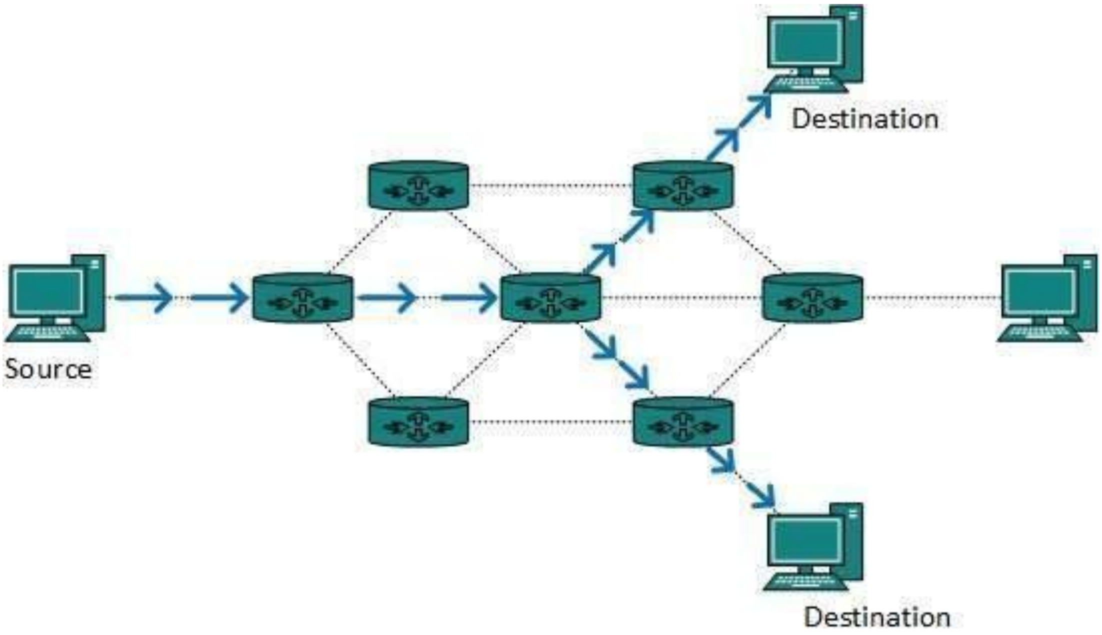


This method is easy on router's CPU but may cause the problem of duplicate packets received from peer routers.

Reverse path forwarding is a technique, in which router knows in advance about its predecessor from where it should receive broadcast. This technique is used to detect and discard duplicates.

Multicast Routing:

Multicast routing is special case of broadcast routing with significance difference and challenges. In broadcast routing, packets are sent to all nodes even if they do not want it. But in Multicast routing, the data is sent to only nodes which wants to receive the packets.

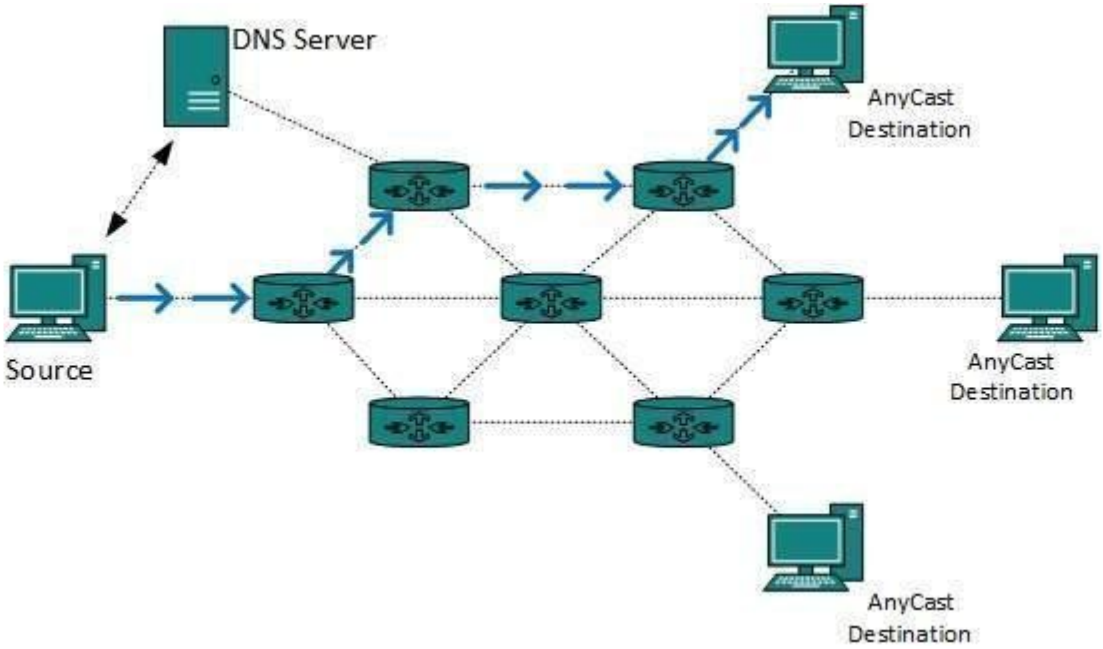


The router must know that there are nodes, which wish to receive multicast packets (or stream) then only it should forward. Multicast routing works spanning tree protocol to avoid looping.

Multicast routing also uses reverse path Forwarding technique, to detect and discard duplicates and loops.

Anycast Routing:

Anycast packet forwarding is a mechanism where multiple hosts can have same logical address. When a packet destined to this logical address is received, it is sent to the host which is nearest in routing topology.



Anycast routing is done with help of DNS server. Whenever an Anycast packet is received it is enquired with DNS to where to send it. DNS provides the IP address which is the nearest IP configured on it.

Unicast Routing Protocols

There are two kinds of routing protocols available to route unicast packets:

- Distance Vector Routing Protocol

Distance Vector is simple routing protocol which takes routing decision on the number of hops between source and destination. A route with less number of hops is considered as the best route. Every router advertises its set best routes to other routers. Ultimately, all routers build up their network topology based on the advertisements of their peer routers,

For example Routing Information Protocol (RIP).

- Link State Routing Protocol

Link State protocol is slightly complicated protocol than Distance Vector. It takes into account the states of links of all the routers in a network. This technique helps routes build a common graph of the entire network. All routers then calculate their best path for routing purposes.for example, Open Shortest Path First (OSPF) and Intermediate System to Intermediate System (ISIS).

Multicast Routing Protocols

Unicast routing protocols use graphs while Multicast routing protocols use trees, i.e. spanning tree to avoid loops. The optimal tree is called shortest path spanning tree.

- **DVMRP** - Distance Vector Multicast Routing Protocol
- **MOSPF** - Multicast Open Shortest Path First
- **CBT** - Core Based Tree
- **PIM** - Protocol independent Multicast
- Protocol Independent Multicast is commonly used now. It has two flavors:
- **PIM Dense Mode**
- This mode uses source-based trees. It is used in dense environment such as LAN.
- **PIM Sparse Mode**
- This mode uses shared trees. It is used in sparse environment such as WAN.

Internet Protocol (IP)

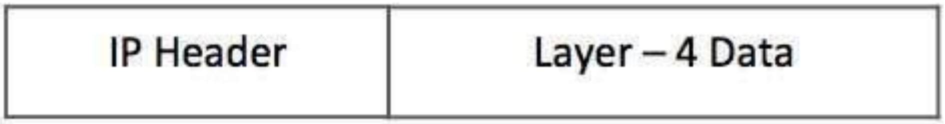
Internet Protocol is connectionless and unreliable protocol. It ensures no guarantee of successfully transmission of data.

In order to make it reliable, it must be paired with reliable protocol such as TCP at the transport layer.

Internet protocol transmits the data in form of a datagram

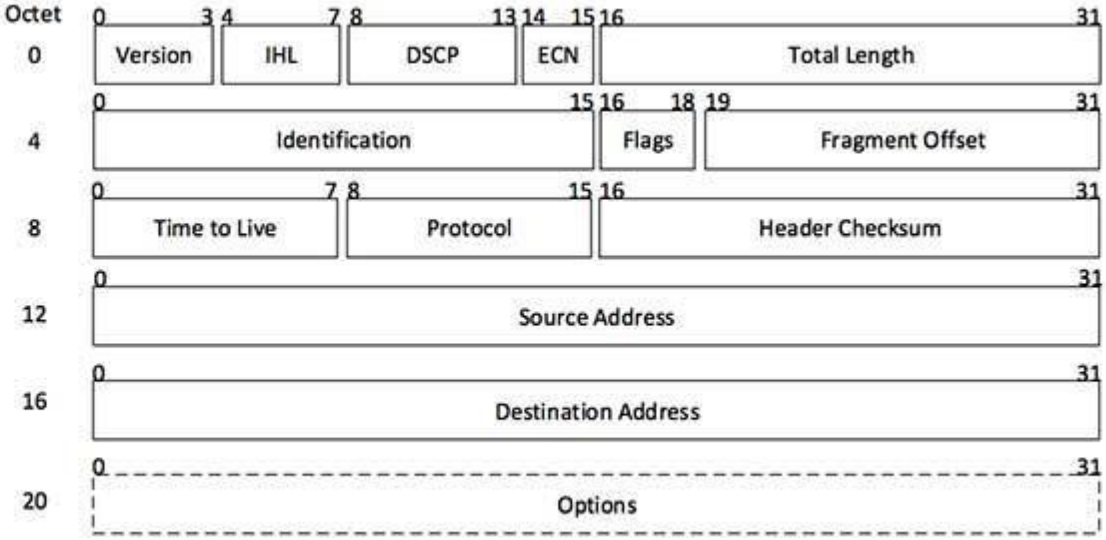
Datagram Format:

Internet Protocol being a layer-3 protocol (OSI) takes data Segments from layer-4 (Transport) and divides it into packets. IP packet encapsulates data unit received from above layer and add to its own header information.



(IP Encapsulation)

The encapsulated data is referred to as IP Payload. IP header contains all the necessary information to deliver the packet at the other end.



[Image: IP Header]

IP header includes many relevant information including Version Number, which, in this context, is 4. Other details are as follows:

- **Version:** Version no. of Internet Protocol used (e.g. IPv4).
- **IHL:** Internet Header Length; Length of entire IP header.
- **DSCP:** Differentiated Services Code Point; this is Type of Service.
- **ECN:** Explicit Congestion Notification; It carries information about the congestion seen in the route.
- **Total Length:** Length of entire IP Packet (including IP header and IP Payload).
- **Identification:** If IP packet is fragmented during the transmission, all the fragments contain same identification number. to identify original IP packet they belong to.
- **Flags:** As required by the network resources, if IP Packet is too large to handle, these „flags‟ tells if they can be fragmented or not. In this 3-bit flag, the MSB is always set to „0‟.

- **Fragment Offset:** This offset tells the exact position of the fragment in the original IP Packet.
- **Time to Live:** To avoid looping in the network, every packet is sent with some TTL value set, which tells the network how many routers (hops) this packet can cross. At each hop, its value is decremented by one and when the value reaches zero, the packet is discarded.
- **Protocol:** Tells the Network layer at the destination host, to which Protocol this packet belongs to, i.e. the next level Protocol. For example protocol number of ICMP is 1, TCP is 6 and UDP is 17.
- **Header Checksum:** This field is used to keep checksum value of entire header which is then used to check if the packet is received error-free.
- **Source Address:** 32-bit address of the Sender (or source) of the packet.
- **Destination Address:** 32-bit address of the Receiver (or destination) of the packet.
- **Options:** This is optional field, which is used if the value of IHL is greater than 5. These options may contain values for options such as Security, Record Route, Time Stamp, etc.

Internet Protocol Version 4 (IPv4)

IPv4 is 32-bit addressing scheme used as TCP/IP host addressing mechanism. IP addressing enables every host on the TCP/IP network to be uniquely identifiable.

IPv4 provides hierarchical addressing scheme which enables it to divide the network into sub-networks, each with well-defined number of hosts. IP addresses are divided into many categories:

- **Class A** - it uses first octet for network addresses and last three octets for host addressing
- **Class B** - it uses first two octets for network addresses and last two for host addressing
- **Class C** - it uses first three octets for network addresses and last one for host addressing
- **Class D** - it provides flat IP addressing scheme in contrast to hierarchical structure for above three.
- **Class E** - It is used as experimental.

IPv4 also has well-defined address spaces to be used as private addresses (not routable on internet), and public addresses (provided by ISPs and are routable on internet).Though IP is not reliable one; it provides „Best-Effort-Delivery" mechanism.

Internet Protocol Version 6 (IPv6)

Exhaustion of IPv4 addresses gave birth to a next generation Internet Protocol version 6. IPv6 addresses its nodes with 128-bit wide address providing plenty of address space for future to be used on entire planet or beyond.

IPv6 has introduced Anycast addressing but has removed the concept of broadcasting. IPv6 enables devices to self-acquire an IPv6 address and communicate within that subnet. This auto-configuration removes the dependability of Dynamic Host Configuration Protocol (DHCP) servers. This way, even if the DHCP server on that subnet is down, the hosts can communicate with each other.

IPv6 provides new feature of IPv6 mobility. Mobile IPv6 equipped machines can roam around without the need of changing their IP addresses.

IPv6 is still in transition phase and is expected to replace IPv4 completely in coming years. At present, there are few networks which are running on IPv6. There are some transition mechanisms available for IPv6 enabled networks to speak and roam around different networks easily on IPv4. These are:

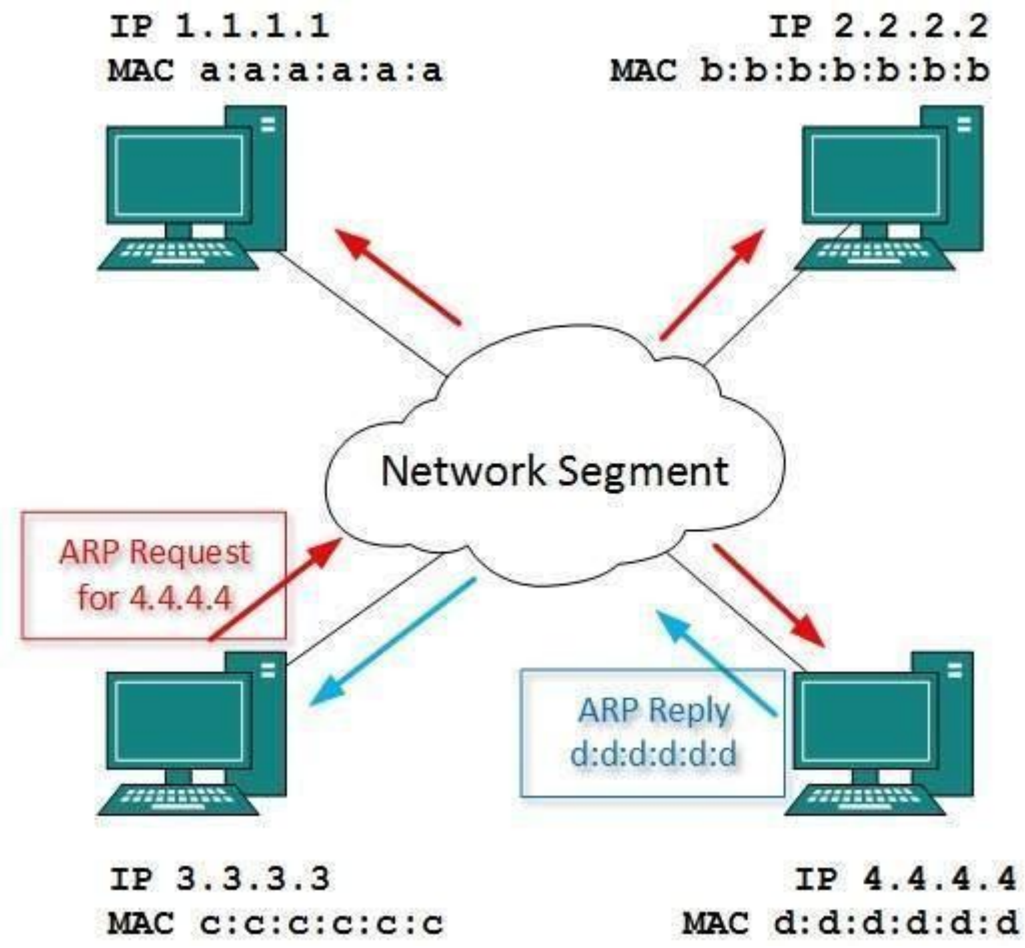
- Dual stack implementation
- Tunneling
- NAT-PT

Internet Controls Protocols:

Address Resolution Protocol (ARP)

While communicating, a host needs Layer-2 (MAC) address of the destination machine which belongs to the same broadcast domain or network. A MAC address is physically burnt into the Network Interface Card (NIC) of a machine and it never changes.

On the other hand, IP address on the public domain is rarely changed. If the NIC is changed in case of some fault, the MAC address also changes. This way, for Layer-2 communication to take place, a mapping between the two is required.



To know the MAC address of remote host on a broadcast domain, a computer wishing to initiate communication sends out an ARP broadcast message asking, “Who has this IP address?” Because it is a broadcast, all hosts on the network segment (broadcast domain) receive this packet and process it. ARP packet contains the IP address of destination host, the sending host wishes to talk to. When a host receives an ARP packet destined to it, it replies back with its own MAC address.

Once the host gets destination MAC address, it can communicate with remote host using Layer-2 link protocol. This MAC to IP mapping is saved into ARP cache of both sending and receiving hosts. Next time, if they require to communicate, they can directly refer to their respective ARP cache.

Reverse ARP is a mechanism where host knows the MAC address of remote host but requires to know IP address to communicate.

Internet Control Message Protocol (ICMP):

ICMP is network diagnostic and error reporting protocol. ICMP belongs to IP protocol suite and uses IP as carrier protocol. After constructing ICMP packet, it is encapsulated in IP packet. Because IP itself is a best-effort non-reliable protocol, so is ICMP.

Any feedback about network is sent back to the originating host. If some error in the network occurs, it is reported by means of ICMP. ICMP contains dozens of diagnostic and error reporting messages.

ICMP-echo and ICMP-echo-reply are the most commonly used ICMP messages to check the reachability of end-to-end hosts. When a host receives an ICMP-echo request, it is bound to send back an ICMP-echo-reply. If there is any problem in the transit network, the ICMP will report that problem.

KarpagamAcademy of Higher Education
(Established Under Section 3 of UGC Act 1956)
Eachanari Post, Coimbatore – 641 021. INDIA
Phone : 0422-2611146, 2611082 Fax No : 0422 -2611043

DEPARTMENT OF COMPUTER APPLICATIONS

BCA (2017-2020 BATCH)

COURSE NAME: COMPUTER NETWORKS **COURSE CODE: 17CAU303**

UNIT IV - POSSIBLE QUESTIONS

PART – A (20 Marks)
(Q.No 1 to 20 Online Examinations)

PART – B
(Each question carries two marks)

1. Define CSMA.
2. Define hub.
3. What is repeater in networking?
4. Define bridges.
5. Define router.
6. What is Ethernet?
7. Define gateway.
8. What is routing?
9. Define IP.
10. Differentiate IPV4 and IPV6.

PART –C
(Each question carries six marks)

1. Explain about CSMA/CD Protocol.
2. Illustrate the IEEE standard for LANS.
3. Discuss about the Gigabit Ethernet
4. Explain i) Hubs ii) Repeaters
5. Explain i) switches ii) bridges
6. Explain the back bone networks

7.Explain about the IPv4 datagram format

8. Illustrate the services and features of Transmission Control Protocol.
9. Elucidate the process- to- process delivery with a neat sketch.
10. Explain the Internet Protocol Version6.

Karpagam Academy of Higher Education

Department of Computer Applications

BCA (2017-2020 Batch)

COMPUTER NETWORKS (17CAU303)

UNIT- IV

S.No	Question	Option1	Option2	Option3	Option4	Answer
1	IP stands for _______	Internet Process	Internet Program	Internet Protocol	Internet Point	Internet Protocol
2	LLC stands for ______	Logical Link Control	Local Link Control	Logical Level Control	Local Level Control	Logical Link Control
3	Lower sub layer of data link layer is responsible for ________	multiple access	point to point access	error detection	flow control	multiple access
4	Multiple-access Protocol is divided into _______ categories	two	three	four	five	three
5	In Carrier Sense Multiple Access (CSMA), if station senses medium before trying to use it then chance of	increased	reduced	highlighted	removed	reduced
6	Code Division Multiple Access (CDMA) differs from Time Division Multiple Access (TDMA) because there is	bandwidth	link	carrier	timesharing	timesharing
7	Protocol that is used to transmit data without any schedule time is ___________	random access	controlled access	channelization	media access	random access
8	Carrier Sense Multiple Access (CSMA) is based on medium called ___________	listen before talk	listen before sending	sense before transmit	sense before collision	sense before transmit
9	Random access is also called the _________	controlled access	channelization	authentication	contention methods	D. contention methods
10	Time-out period is equal to maximum possible propagation delay of	Square-trip	Round-trip	Rectangular-trip	Triangle-trip	B. Round-trip
11	Field of MAC frame that alerts receiver and enables it to synchronize is known as	SFD	preamble	source address	destination address	B. preamble
12	TCP stands for _______	Transmission Control Protocol	Transfer Control Protocol	Transition Control Protocol	Transaction Control Protocol	Transaction Control Protocol
13	UDP stands for ________	Universal Datagram Protocol	User Datagram Protocol	Universal Datagram Packet	User Datagram Packet	User Datagram Protocol
14	ISN stands for _____	Initial Standard Number	Initial Sequence Number	Initial Socket Number	Initial Server Number	Initial Sequence Number
15	The Client program issues a request for an ________	active open	passive open	passive close	active close	active open
16	Ethernet was created in ________.	1974	1975	1976	1977	1976
17	Ethernet has gone through _______ generations.	1	2	3	4	4

18	A _______ is a device that operates only in both physical and data link layers of the Internet model	hub	repeater	bridge	switch	switch
19	A _______ is a device that operates only in the physical layer of the Internet model	hub	repeater	bridge	switch	repeater
20	A _______ is a device that operates only in the physical , data link and network layers of the Internet model	hub	router	bridge	switch	router
21	________ is a device that operates at all the five layers	gateway	hub	bridge	switch	gateway
22	An IPv4 address is ______ long.	16 bits	32 bits	64 bits	128 bits	32 bits
23	How many classes in IPv4 addresses?	2	3	4	5	5
24	Packets in the IPv4 layer are called ______	datagrams	segments	frames	stream of bits	datagrams
25	_______ defines a device’s connection to a network.	MAC Address	IP Address	Network Address	Local address	IP Address
26	Addresses in _______ are used for multicast communication.	Class A	Class B	Class C	Class D	Class D
27	A __________ has a table used in filtering decisions	hub	repeater	bridge	switch	bridge
28	A bridge does not change the ________ addresses in a frame	physical	logical	network	local	logical
29	In graph theory, _________ is a graph in which there is no loop.	decision tree	spanning tree	binary tree	b-tree	spanning tree
30	A three layer switch is a ______	hub	router	bridge	switch	router
31	A two layer switch is a _________	hub	router	bridge	switch	bridge
32	Communication at network layer in the internet is .	connectionless	point-to-point	connection oriented	packet-switched	connectionless
33	What is the abbrevation for IPV4_______.	Inter Protocol Versus 4	Inter Position Version 4	Internet protocol version 4	Internet Position Versus 4	Internet protocol version 4
34	IPV4 provides the term 'best-effort' means that .	no error control	error control	error detection	datagram	no error control
35	Packets in the IPV4 layer are called______.	frames	datagroup	switching	datagrams	datagrams
36	A datagram is a variable length packet consisting of______parts.	one	six	two	three	two
37	An IPv6 address is_______bits long.	128	126	125	127	128
38	In classless addressing,atleast_______columns in a routing table.	5	6	3	4	4
39	The maximum length of datagram is _______	512 bytes	1024 bytes	2048 bytes	65,535 bytes	65,535 bytes
40	__________algorithm creates a shortest path tree from a graph.	data	dakstra	define	dijkstra	dijkstra
41	_________layer is responsible for process-to-process delivery.	transport	physical	application	network	transport
42	Internet has decided to use universal port numbers for severs called .	well-unknown port	well-known port	well-known protocol	well-unknown process	well-known port
43	IANA has divided the port numbers into_______ranges.	six	four	five	three	three
44	_______a connection,is first established between the sender and receiver.	connection-oriented	connectionless	token	dialog	connection-oriented
45	UDP is called___________.	connection-oriented	check point	token	connetionless	connetionless
46	UDP length = IP length - ________.	IP length	IP breadth	IP header's length	IP header's breadth	IP header's length
47	UDP is a suitable transport protocol for________.	unicasting	multicasting	nocasting	broadcasting	multicasting
48	TCP groups a number of bytes together into a packet called .	segment	encapsulation	datagram	data binding	segment
49	The acknowledgement number is ________.	natural	whole	integers	cumulative	cumulative
50	_________ flag is used to terminate the connection.	TER	FIN	URG	PSH	FIN

Transport Layer Functions and Protocols:

Transport Services:

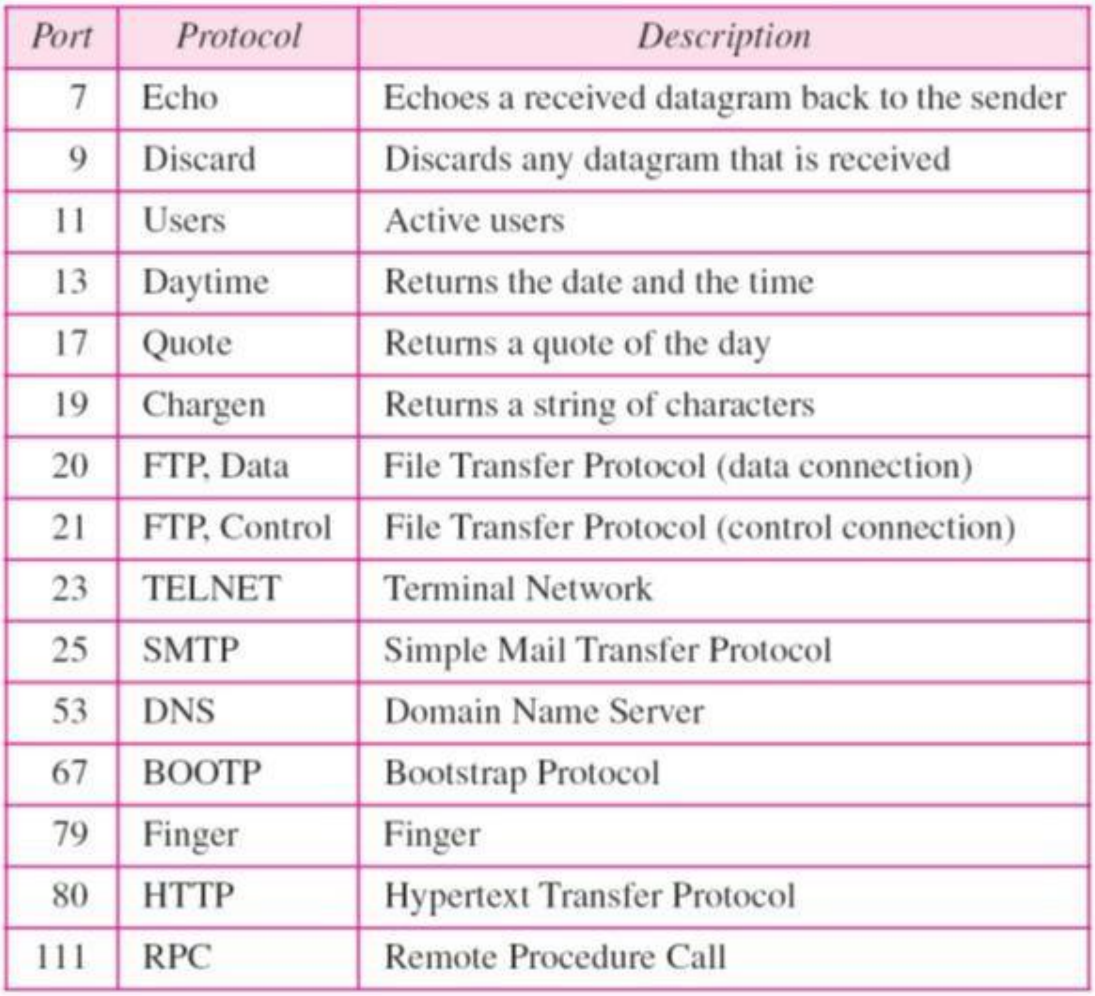
The second transport layer protocol is called Transmission Control Protocol (TCP). TCP, like UDP, is a process-to-process (program-to-program) protocol. TCP, therefore, like UDP, uses port numbers. Unlike UDP, TCP is a connection oriented protocol; it creates a virtual connection between two TCPs to send data. In addition, TCP uses flow and error control mechanisms at the transport level.

TCP Services:

The services offered by TCP to the processes at the application layer are as follows:

Process-to-Process Communication:

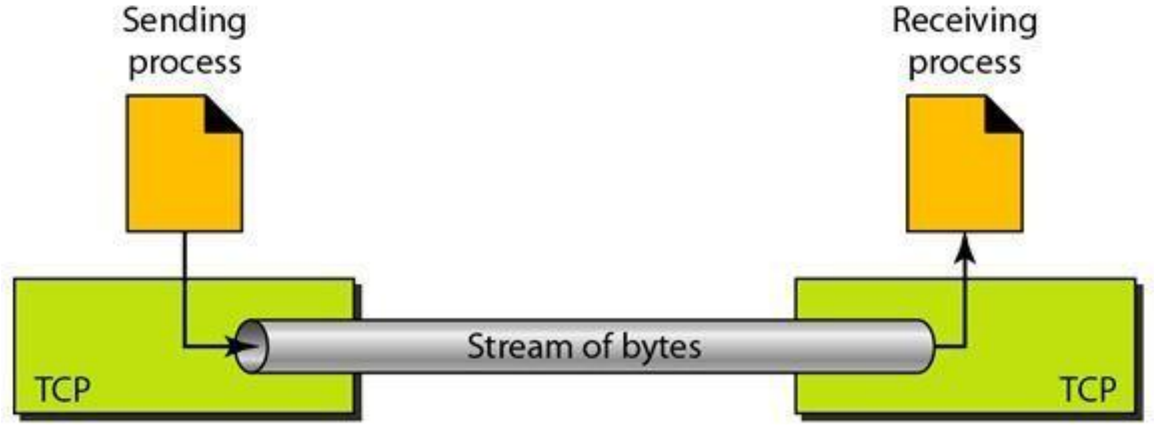
TCP provides process-to-process communication using port numbers. The following table lists some well-known port numbers used by TCP.



Port	*Protocol*	*Description*
7	Echo	Echoes a received datagram back to the sender
9	Discard	Discards any datagram that is received
11	Users	Active users
13	Daytime	Returns the date and the time
17	Quote	Returns a quote of the day
19	Chargen	Returns a string of characters
20	FTP, Data	File Transfer Protocol (data connection)
21	FTP, Control	File Transfer Protocol (control connection)
23	TELNET	Terminal Network
25	SMTP	Simple Mail Transfer Protocol
53	DNS	Domain Name Server
67	BOOTP	Bootstrap Protocol
79	Finger	Finger
80	HTTP	Hypertext Transfer Protocol
111	RPC	Remote Procedure Call

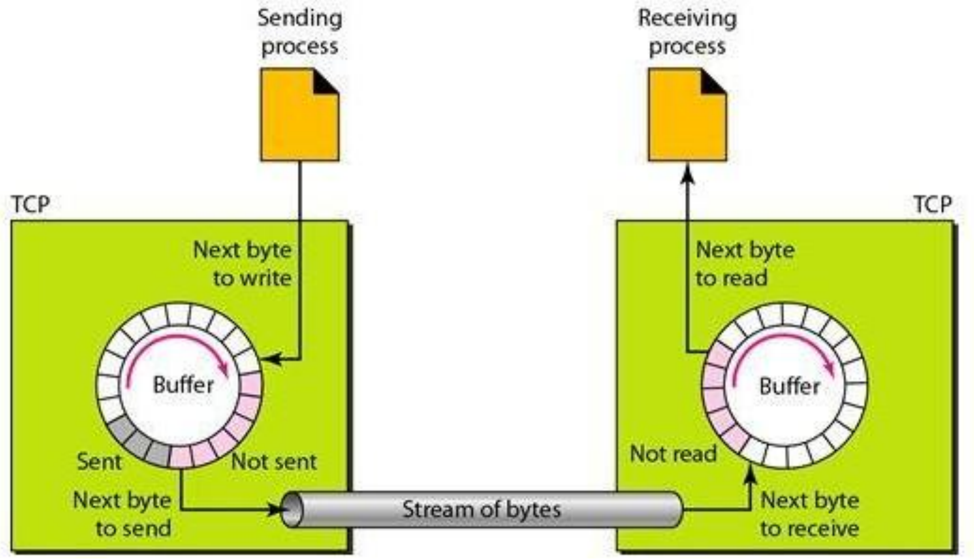
Stream Delivery Service:

TCP, unlike UDP, is a stream-oriented protocol. TCP, on the other hand, allows the sending process to deliver data as a stream of bytes and allows the receiving process to obtain data as a stream of bytes. TCP creates an environment in which the two processes seem to be connected by an imaginary "tube" that carries their data across the Internet. This imaginary environment is depicted in the following figure. The sending process produces (writes to) the stream of bytes, and the receiving process consumes (reads from) them.



Sending and Receiving Buffers:

Because the sending and the receiving processes may not write or read data at the same speed, TCP needs buffers for storage. There are two buffers, the sending buffer and the receiving buffer, one for each direction and these buffers are also necessary for flow and error control mechanisms used by TCP.) One way to implement a buffer is to use a circular array of 1-byte locations as shown in the following figure.



The above figure shows the movement of the data in one direction.

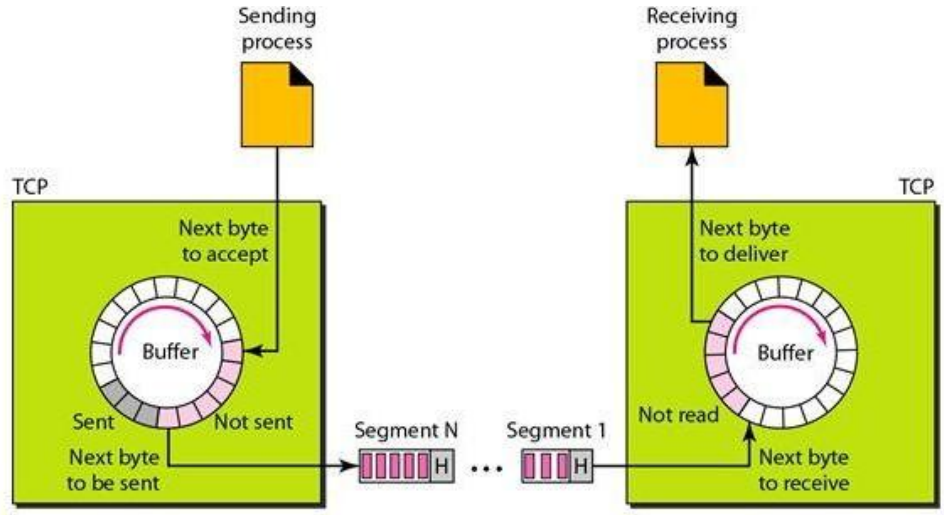
At the sending site, the buffer has three types of chambers. The white section contains empty chambers that can be filled by the sending process (producer). The gray area holds bytes that have been sent but not yet acknowledged. TCP keeps these bytes in the buffer until it receives an acknowledgment. The colored area contains bytes to be sent by the sending TCP. However, TCP may be able to send only part of this colored section. This could be due to the slowness of the receiving process or perhaps to congestion in the network. Also note that after the bytes in the gray chambers are acknowledged, the chambers are recycled and available for use by the sending process. This is why we show a circular buffer.

At the receiving site, the operation of the buffer at the receiver site is simpler. The circular buffer is divided into two areas (shown as white and colored). The white area contains empty chambers to be filled by bytes received from the network. The colored sections contain received bytes that can be read by the receiving process. When a byte is read by the receiving process, the chamber is recycled and added to the pool of empty chambers.

Segments:

The buffering handles the disparity between the speed of the producing and consuming processes, we need one more step before we can send data. The IP layer, as a service provider for TCP, needs to send data in packets, not as a stream of bytes. At the transport layer, TCP groups a number of bytes together into a packet called a segment. TCP adds a header to each segment (for control purposes) and delivers the segment to the IP layer for transmission.

The segments are encapsulated in IP datagrams and transmitted. This entire operation is transparent to the receiving process. The segments may be received out of order, lost, or corrupted and resent. All these are handled by TCP with the receiving process unaware of any activities. The following figure shows how segments are created from the bytes in the buffers.



Full-Duplex Communication:

TCP offers full-duplex service, in which data can flow in both directions at the same time. Each TCP then has a sending and receiving buffer, and segments move in both directions.

TCP, unlike UDP, is a connection-oriented protocol. When a process at site A wants to send and receive data from another process at site B, the following occurs:

1. The two TCPs establish a connection between them.

2. Data are exchanged in both directions.

3. The connection is terminated.

The TCP segment is encapsulated in an IP datagram and can be sent out of order, or lost, or corrupted, and then resent. Each may use a different path to reach the destination. There is no physical connection. TCP creates a stream-oriented environment in which it accepts the responsibility of delivering the bytes in order to the other site.

Reliable Service

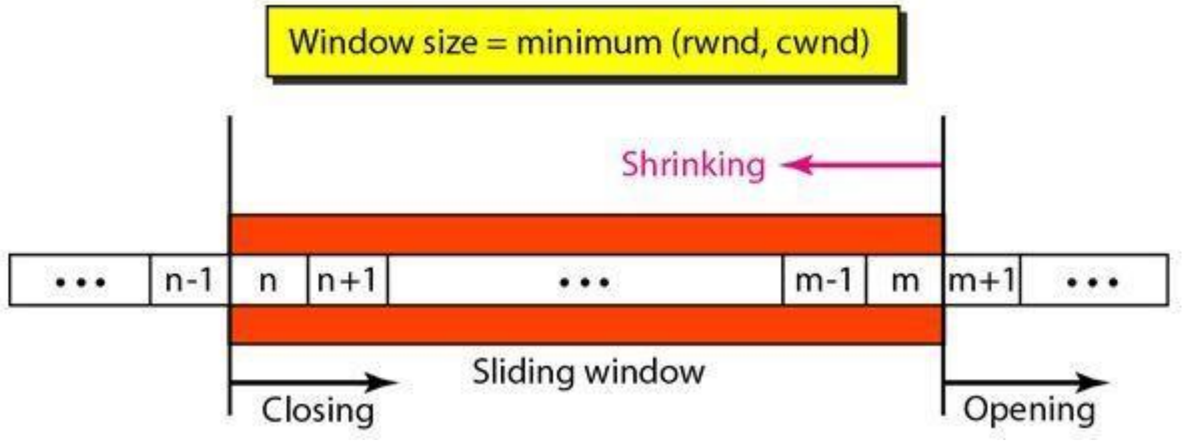
TCP is a reliable transport protocol. It uses an acknowledgment mechanism to check the safe and sound arrival of data. We will discuss this feature further in the section on error control.

Flow Control in TCP:

TCP uses a sliding window to handle flow control. The sliding window protocol used by TCP, however, is something between the Go-Back-N and Selective Repeat sliding window.

There are two big differences between this sliding window and the one we used at the data link layer. First, the sliding window of TCP is byte-oriented but data link layer sliding window is frame-oriented. Second, the TCP's sliding window is of variable size and the data link layer was of fixed size.

The following figure shows the sliding window in TCP.



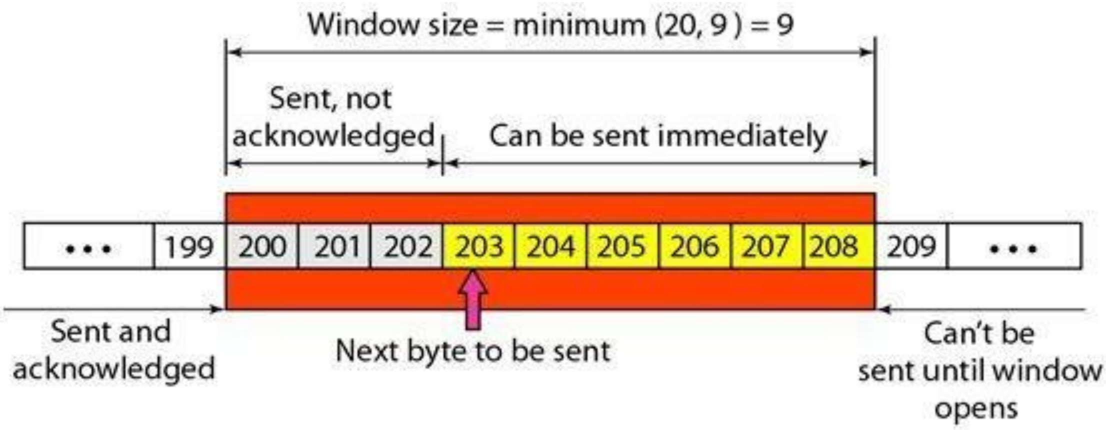
The window spans a portion of the buffer containing bytes received from the process. The bytes inside the window are the bytes that can be in transit; they can be sent without worrying about acknowledgment. The imaginary window has two walls: one left and one right.

The window is opened, closed, or shrunk. These three activities, as we will see, are in the control of the receiver (and depend on congestion in the network), not the sender. The sender must obey the commands of the receiver in this matter.

Opening a window means moving the right wall to the right. This allows more new bytes in the buffer that are eligible for sending. Closing the window means moving the left wall to the right. This means that some bytes have been acknowledged and the sender need not worry about them anymore. Shrinking the window means moving the right wall to the left. This is not allowed in some implementations because it means revoking the eligibility of some bytes for sending.

The size of the window at one end is determined by the lesser of two values: receiver window (rwnd) or congestion window (cwnd). The receiver window is the value advertised by the opposite end in a segment containing acknowledgment. It is the number of bytes the other end can accept before its buffer overflows and data are discarded. The congestion window is a value determined by the network to avoid congestion.

The following figure shows an unrealistic example of a sliding window.



The sender has sent bytes up to 202. We assume that cwnd is 20 (in reality this value is thousands of bytes). The receiver has sent an acknowledgment number of 200 with an rwnd of 9 bytes (in reality this value is thousands of bytes).

The size of the sender window is the minimum of rwnd and cwnd, or 9 bytes. Bytes 200 to 202 are sent, but not acknowledged. Bytes 203 to 208 can be sent without worrying about acknowledgment. Bytes 209 and above cannot be sent.

Features of TCP sliding window are as follows:

- The size of the window is the lesser of rwnd and cwnd.

- The source does not have to send a full window's worth of data.

- The window can be opened or closed by the receiver, but should not be shrunk.

- The destination can send an acknowledgment at any time as long as it does not result in a shrinking window.

- The receiver can temporarily shut down the window; the sender, however, can always send a segment of 1 byte after the window is shut down.

Error Control in TCP:

TCP is a reliable transport layer protocol. This means that an application program that delivers a stream of data to TCP relies on TCP to deliver the entire stream to the application program on the other end in order, without error, and without any part lost or duplicated.

TCP provides reliability using error control. Error control includes mechanisms for detecting corrupted segments, lost segments, out-of-order segments, and duplicated segments. Error control also includes a mechanism for correcting errors after they are detected. Error detection and correction in TCP is achieved through the use of three simple tools: checksum, acknowledgment, and time-out.

1. Checksum:

Each segment includes a checksum field which is used to check for a corrupted segment. If the segment is corrupted, it is discarded by the destination TCP and is considered as lost. TCP uses a 16-bit checksum that is mandatory in every segment.

2. Acknowledgment:

TCP uses acknowledgments to confirm the receipt of data segments. Control segments that carry no data but consume a sequence number are also acknowledged. ACK segments are never acknowledged.

3. Retransmission:

The heart of the error control mechanism is the retransmission of segments. When a segment is corrupted, lost, or delayed, it is retransmitted. A segment is retransmitted on two occasions: when a retransmission timer expires or when the sender receives three duplicate ACKs.

Retransmission After RTO:

A recent implementation of TCP maintains one retransmission time-out (RTO) timer for all outstanding (sent, but not acknowledged) segments.

When the timer matures, the earliest outstanding segment is retransmitted even though lack of a received ACK can be due to a delayed segment, a delayed ACK, or a lost acknowledgment. Note that no time-out timer is set for a segment that carries only an acknowledgment. The value of RTO is dynamic in TCP and is updated based on the round-trip time (RTT) of segments. An RTI is the time needed for a segment to reach a destination and for an acknowledgment to be received.

Retransmission After Three Duplicate ACK Segments:

The previous rule about retransmission of a segment is sufficient if the value of RTO is not very large. Sometimes, however, one segment is lost and the receiver receives so many out-of-order segments that they cannot be saved (limited buffer size). To avoid this situation, most implementations today follow the three-duplicate-ACKs rule and retransmit the missing segment immediately. This feature is referred to as fast retransmission.

Out-of-Order Segments:

When a segment is delayed, lost, or discarded, the segments following that segment arrive out of order. The out-of-order segments are stored temporarily and flag them as out-of-order segments until the missing segment arrives. Note, however, that the out-of-order segments are not delivered to the process. TCP guarantees that data are delivered to the process in order.

Lost Segment:

A lost segment and a corrupted segment are treated the same way by the receiver. A lost segment is discarded somewhere in the network; a corrupted segment is discarded by the receiver itself. Both are considered lost.

Fast Retransmission:

In this example, If RTO has a higher value and receiver receives the fourth, fifth, and sixth segments, it triggers an acknowledgment. The sender receives four acknowledgments with the same value (three duplicates). Although the timer for segment 3 has not matured yet, the fast transmission requires that segment 3, the segment that is expected by all these acknowledgments, be resent immediately.

Note that only one segment is retransmitted although four segments are not acknowledged. When the sender receives the retransmitted ACK, it knows that the four segments are safe and sound because acknowledgment is cumulative.

Connection Establishment and Release:

TCP is connection-oriented. A connection-oriented transport protocol establishes a virtual path between the source and destination. All the segments belonging to a message are then sent over this virtual path. Using a single virtual pathway for the entire message facilitates the acknowledgment process as well as retransmission of damaged or lost frames.

In TCP, connection-oriented transmission requires three phases:

1. Connection establishment

2. Data transfer

3. Connection termination.

Connection Establishment:

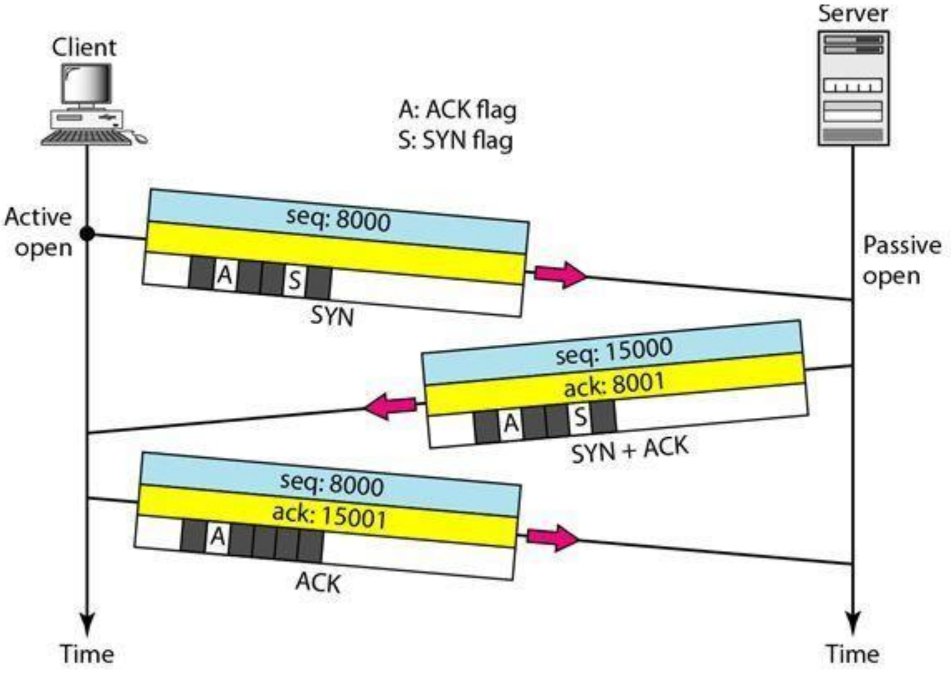
TCP transmits data in full-duplex mode. When two TCPs in two machines are connected, they are able to send segments to each other simultaneously. This implies that each party must initialize communication and get approval from the other party before any data are transferred.

Three-Way Handshaking:

The connection establishment in TCP is called three way handshaking. In our example, an application program, called the client, wants to make a connection with another application program, called the server, using TCP as the transport layer protocol.

The process starts with the server. The server program tells its TCP that it is ready to accept a connection. This is called a request for a passive open. Although the server TCP is ready to accept any connection from any machine in the world, it cannot make the connection itself.

The client program issues a request for an active open. A client that wishes to connect to an open server tells its TCP that it needs to be connected to that particular server. TCP can now start the three-way handshaking process as shown in the following figure.



To show the process, we use two time lines, one at each site. Each segment has values for all its header fields and perhaps for some of its option fields, too.

We show the sequence number, the acknowledgment number, the control flags (only those that are set), and the window size, if not empty. The three steps in this phase are as follows.

1. The client sends the first segment, a SYN segment, in which only the SYN flag is set. This segment is for synchronization of sequence numbers. It consumes one sequence number. When the data transfer starts, the sequence number is incremented by 1. We can say that the SYN segment carries no real data, but we can think of it as containing 1 imaginary byte.

2. The server sends the second segment, a SYN +ACK segment, with 2 flag bits set, SYN and ACK. This segment has a dual purpose. It is a SYN segment for communication in the other direction and serves as the acknowledgment for the SYN segment. It consumes one sequence number.

3. The client sends the third segment. This is just an ACK segment. It acknowledges the receipt of the second segment with the ACK flag and acknowledgment number field. Note that the sequence number in this segment is the same as the one in the SYN segment; the ACK segment does not consume any sequence numbers.

SYN Flooding Attack:

The connection establishment procedure in TCP is susceptible to a serious security problem called the SYN flooding attack. This happens when a malicious attacker sends a large number of SYN segments to a server, pretending that each of them is corning from a different client by faking the source IP addresses in the datagrams.

The server, assuming that the clients are issuing an active open, allocates the necessary resources, such as creating communication tables and setting timers. The TCP server then sends the SYN +ACK segments to the fake clients, which are lost.

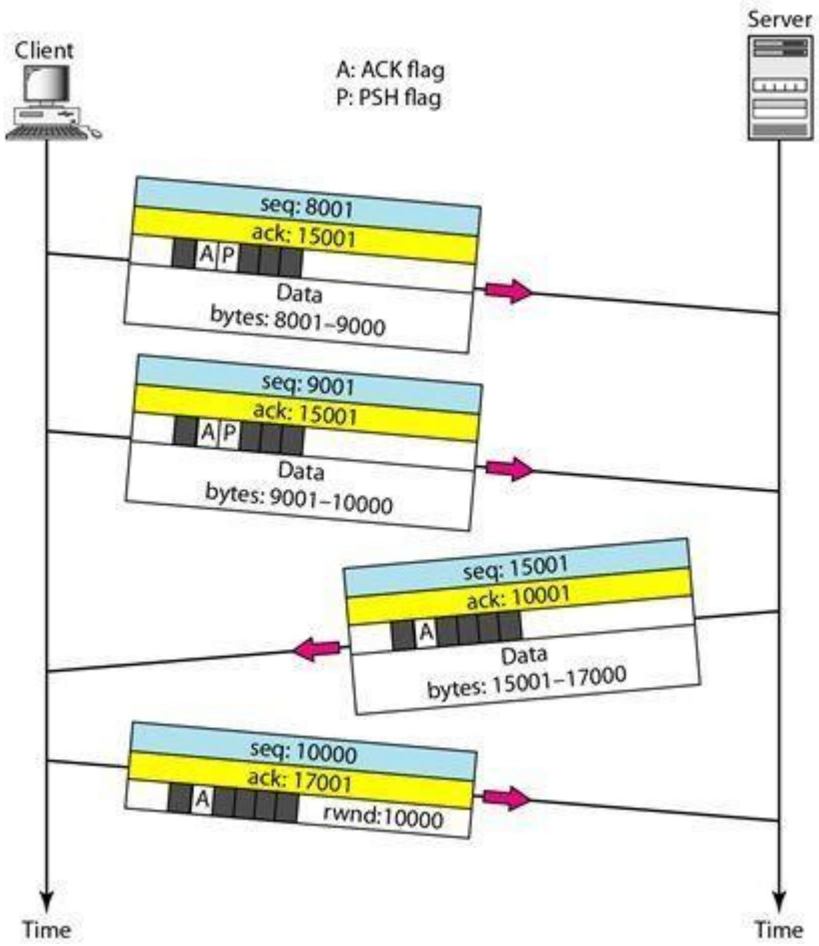
During this time, however, a lot of resources are occupied without being used. If, during this short time, the number of SYN segments is large, the server eventually runs out of resources and may crash. This SYN flooding attack belongs to a type of security attack known as a denial-of-service attack.

Some implementations of TCP have strategies to alleviate the effects of a SYN attack. Some have imposed a limit on connection requests during a specified period of time. Others filter out datagrams coming from unwanted source addresses. One recent strategy is to postpone resource allocation until the entire connection is set up, using what is called a cookie.

Data Transfer:

After connection is established, bidirectional data transfer can take place. The client and server can both send data and acknowledgments. In this example, after connection is established (not shown in the figure), the client sends 2000 bytes of data in two segments. The server then sends 2000 bytes in one segment. The client sends one more segment. The first three segments carry both data and acknowledgment, but the last segment carries only an acknowledgment because there are no more data to be sent. Note the values of the sequence and acknowledgment numbers.

The data segments sent by the client have the PSH (push) flag set so that the server TCP knows to deliver data to the server process as soon as they are received. The segment from the server, on the other hand, does not set the push flag. Most TCP implementations have the option to set or not set this flag.



Pushing Data:

The sending TCP uses a buffer to store the stream of data coming from the sending application program. The sending TCP can select the segment size. The receiving TCP also buffers the data when they arrive and delivers them to the application program when the application program is ready or when it is convenient for the receiving TCP. This type of flexibility increases the efficiency of TCP.

But on some occasions the application program has no need for this flexibility. For example, the application program on one site wants to send a keystroke to the application at the other site and receive an immediate response. Delayed transmission and delayed delivery of data may not be acceptable by the application program.
TCP can handle such a situation. The application program at the sending site can request a push operation. This means that the sending TCP must not wait for the window to be filled. It must create a segment and send it immediately. The sending TCP must also set the push bit (PSH) to let the receiving TCP know that the segment includes data that must be delivered to the receiving application program as soon as possible and not to wait for more data to come.

Urgent Data:

TCP is a stream-oriented protocol. This means that the data are presented from the application program to TCP as a stream of bytes. Each byte of data has a position in the stream. However, on occasion an application program needs to send urgent bytes. This means that the sending application program wants a piece of data to be read out of order by the receiving application program.

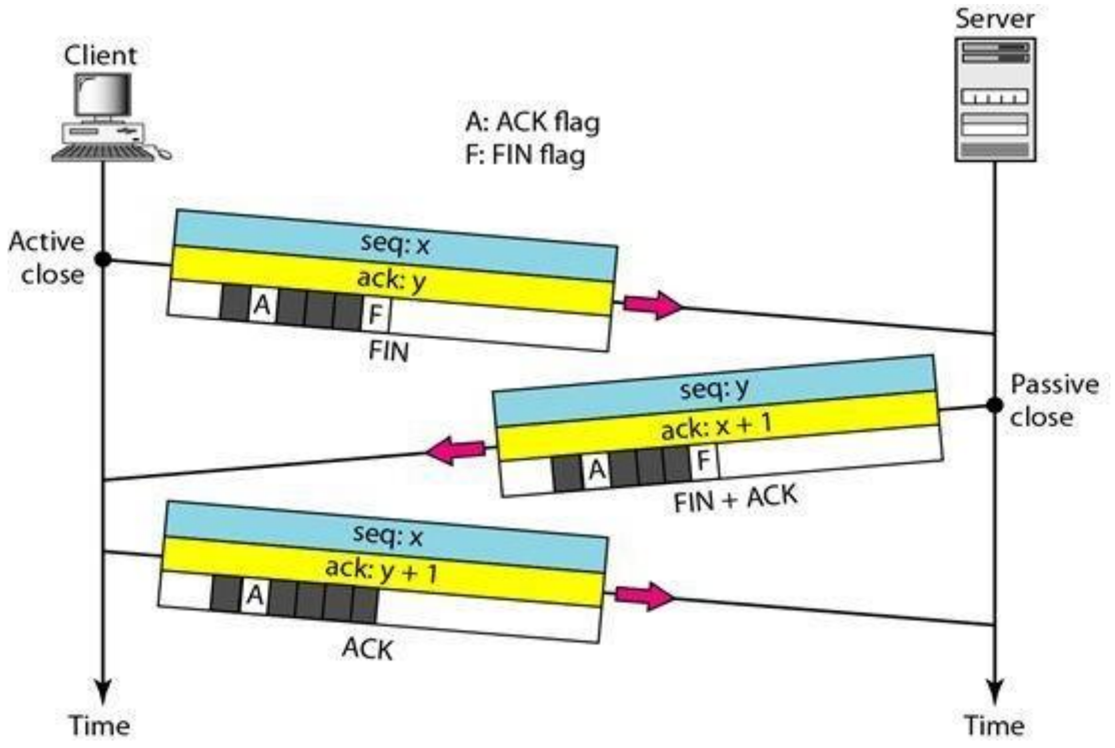
The solution is to send a segment with the URG bit set. The sending application program tells the sending TCP that the piece of data is urgent. The sending TCP creates a segment and inserts the urgent data at the beginning of the segment. The rest of the segment can contain normal data from the buffer. The urgent pointer field in the header defines the end of the urgent data and the start of normal data.

When the receiving TCP receives a segment with the URG bit set, it extracts the urgent data from the segment, using the value of the urgent pointer, and delivers them, out of order, to the receiving application program..

Connection Termination:

Any of the two parties involved in exchanging data (client or server) can close the connection, although it is usually initiated by the client. There are two options for connection termination: three-way handshaking and four-way handshaking with a half-close option.

Three-Way Handshaking: The three-way handshaking for connection termination as shown in the following figure.



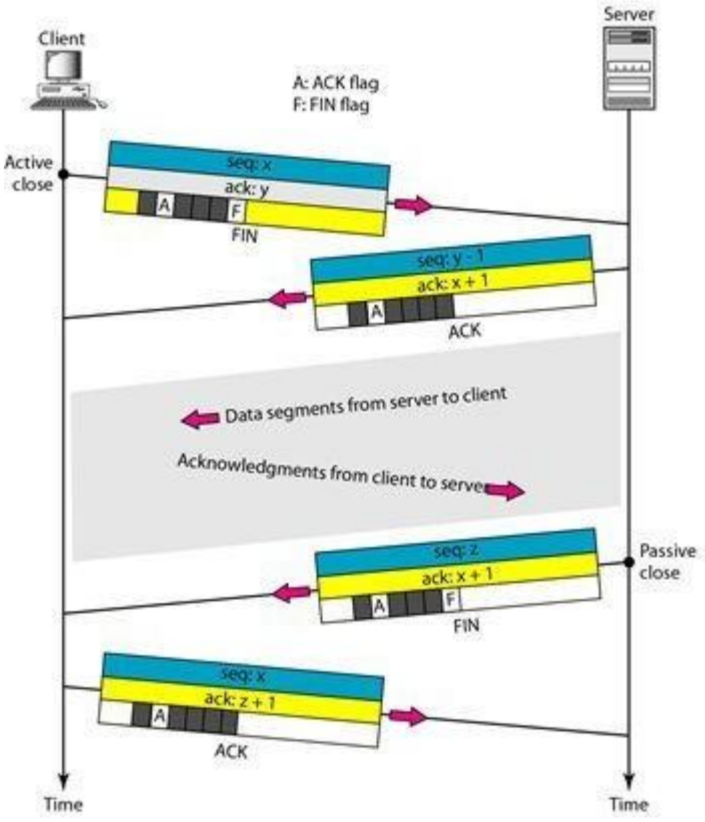
1. In a normal situation, the client TCP, after receiving a close command from the client process, sends the first segment, a FIN segment in which the FIN flag is set. Note that a FIN segment can include the last chunk of data sent by the client, or it can be just a control segment as shown in the above figure. If it is only a control segment, it consumes only one sequence number.

2. The server TCP, after receiving the FIN segment, informs its process of the situation and sends the second segment, a FIN +ACK segment, to confirm the receipt of the FIN segment from the client and at the same time to announce the closing of the connection in the other direction. This segment can also contain the last chunk of data from the server. If it does not carry data, it consumes only one sequence number.

3. The client TCP sends the last segment, an ACK segment, to confirm the receipt of the FIN segment from the TCP server. This segment contains the acknowledgment number, which is 1 plus the sequence number received in the FIN segment from the server. This segment cannot carry data and consumes no sequence numbers.

Half-Close: In TCP, one end can stop sending data while still receiving data. This is called a half-close. It can occur when the server needs all the data before processing can begin.

A good example is sorting. When the client sends data to the server to be sorted, the server needs to receive all the data before sorting can start. This means the client, after sending all the data, can close the connection in the outbound direction. However, the inbound direction must remain open to receive the sorted data. The server, after receiving the data, still needs time for sorting; its outbound direction mustmain open. The following figure shows an example of a half-close.



The client half-closes the connection by sending a FIN segment. The server accepts the half-close by sending the ACK segment.

The data transfer from the client to the server stops. The server, however, can still send data. When the server has sent all the processed data, it sends a FIN segment, which is acknowledged by an ACK from the client. After half-closing of the connection, data can travel from the server to the client and acknowledgments can travel from the client to the server. The client cannot send any more data to the server.

When the retransmission timer for a packet expires, or four duplicate SACKs arrive that declare a packet as missing the chunks in that packet are moved to the retransmission queue to be resent. These chunks are considered lost, rather than outstanding. The chunks in the retransmission queue have priority

Overview of Application and Protocols:

Overview of DNS Protocol:

When **DNS** was not into existence, one had to download a **Host file** containing host names and their corresponding IP address. But with increase in number of hosts of internet, the size of host file also increased. This resulted in increased traffic on downloading this file. To solve this problem the DNS system was introduced.

Domain Name System helps to resolve the host name to an address. It uses a hierarchical naming scheme and distributed database of IP addresses and associated names

IP Address

IP address is a unique logical address assigned to a machine over the network. An IP address exhibits the following properties:

- IP address is the unique address assigned to each host present on Internet.
- IP address is 32 bits (4 bytes) long.
- IP address consists of two components: **network component** and **host component**.
- Each of the 4 bytes is represented by a number from 0 to 255, separated with dots. For example 137.170.4.124

IP address is 32-bit number while on the other hand domain names are easy to remember names. For example, when we enter an email address we always enter a symbolic string such as webmaster@tutorialspoint.com.

Uniform Resource Locator (URL)

Uniform Resource Locator (URL) refers to a web address which uniquely identifies a document over the internet.

This document can be a web page, image, audio, video or anything else present on the web. For example, **www.tutorialspoint.com/internet_technology/index.html** is an URL to the index.html which is stored on tutorialspoint web server under internet_technology directory.

URL Types

There are two forms of URL as listed below:

1. Absolute URL
2. Relative URL

Absolute URL

Absolute URL is a complete address of a resource on the web. This completed address comprises of protocol used, server name, path name and file name.

For example http:// www.tutorialspoint.com / internet_technology /index.htm. where:

- **http** is the protocol.
- **tutorialspoint.com** is the server name.
- **index.htm** is the file name.

The protocol part tells the web browser how to handle the file. Similarly we have some other protocols also that can be used to create URL are:

- FTP
- https
- Gopher
- mailto
- news

Relative URL

Relative URL is a partial address of a webpage. Unlike absolute URL, the protocol and server part are omitted from relative URL.

Relative URLs are used for internal links i.e. to create links to file that are part of same website as the WebPages on which you are placing the link.

For example, to link an image on tutorialspoint.com/internet_technology/internet_referemce_models, we can use the relative URL which can take the form like **/internet_technologies/internet-osi_model.jpg.**

Difference between Absolute and Relative URL

Absolute URL	**Relative URL**
Used to link web pages on different websites	Used to link web pages within the same website.
Difficult to manage.	Easy to Manage
Changes when the server name or	Remains same even of we change the server name

directory name changes	or directory name.
Take time to access	Comparatively faster to access.

Domain Name System Architecture

The Domain name system comprises of **Domain Names, Domain Name Space, Name Server** that have been described below:

Domain Names

Domain Name is a symbolic string associated with an IP address. There are several domain names available; some of them are generic such as **com, edu, gov, net**etc, while some country level domain names such as **au, in, za, us** etc.

The following table shows the **Generic** Top-Level Domain names:

Domain Name	Meaning
Com	Commercial business
Edu	Education
Gov	U.S. government agency
Int	International entity
Mil	U.S. military
Net	Networking organization
Org	Non profit organization

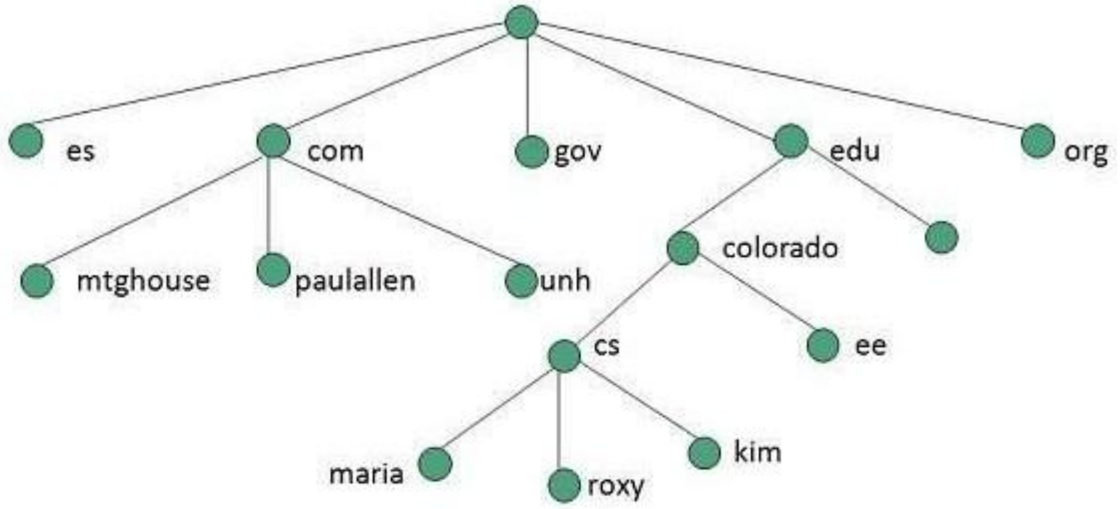
The following table shows the **Country top-level** domain names:

Domain Name	Meaning
au	Australia

in	India
cl	Chile
fr	France
us	United States
za	South Africa
uk	United Kingdom
jp	Japan
es	Spain
de	Germany
ca	Canada
ee	Estonia
hk	Hong Kong

Domain Name Space

The domain name space refers a hierarchy in the internet naming structure. This hierarchy has multiple levels (from 0 to 127), with a root at the top. The following diagram shows the domain name space hierarchy:



In the above diagram each subtree represents a domain. Each domain can be partitioned into sub domains and these can be further partitioned and so on.

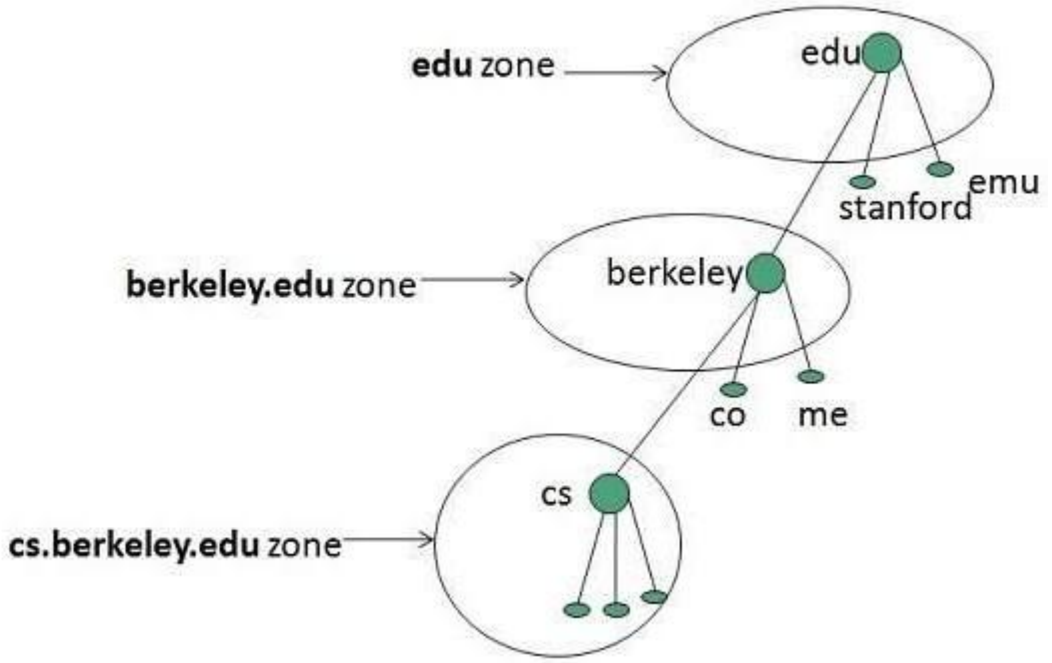
Name Server

Name server contains the DNS database. This database comprises of various names and their corresponding IP addresses. Since it is not possible for a single server to maintain entire DNS database, therefore, the information is distributed among many DNS servers.

- Hierarchy of server is same as hierarchy of names.
- The entire name space is divided into the zones

Zones

Zone is collection of nodes (sub domains) under the main domain. The server maintains a database called zone file for every zone.



If the domain is not further divided into sub domains then domain and zone refers to the same thing.

The information about the nodes in the sub domain is stored in the servers at the lower levels however; the original server keeps reference to these lower levels of servers.

Types of Name Servers

Following are the three categories of Name Servers that manages the entire Domain Name System:

1. Root Server
2. Primary Server
3. Secondary Server

Root Server

Root Server is the top level server which consists of the entire DNS tree. It does not contain the information about domains but delegates the authority to the other server

Primary Servers

Primary Server stores a file about its zone. It has authority to create, maintain, and update the zone file.

Secondary Server

Secondary Server transfers complete information about a zone from another server which may be primary or secondary server. The secondary server does not have authority to create or update a zone file.

DNS Working

DNS translates the domain name into IP address automatically. Following steps will take you through the steps included in domain resolution process:

- When we type **www.tutorialspoint.com** into the browser, it asks the local DNS Server for its IP address.

  Here the local DNS is at ISP end.
- When the local DNS does not find the IP address of requested domain name, it forwards the request to the root DNS server and again enquires about IP address of it.
- The root DNS server replies with delegation that **I do not know the IP address of www.tutorialspoint.com but know the IP address of DNS Server.**
- The local DNS server then asks the com DNS Server the same question.
- The **com** DNS Server replies the same that it does not know the IP address of www.tutorialspont.com but knows the address of tutorialspoint.com.
- Then the local DNS asks the tutorialspoint.com DNS server the same question.
- Then tutorialspoint.com DNS server replies with IP address of www.tutorialspoint.com.
- Now, the local DNS sends the IP address of www.tutorialspoint.com to the computer that sends the request.

Overview of WWW and HTTP Protocol:

The WWW is the brainchild of Tim Berners Lee a CERN who had the idea of creating an electronic web of research information. The web is currently the fastest growing Internet information system, with new resources being added regularly. The web relies on a set of protocols, conventions and software to operate. The web is a distributed system of delivering linked documents over the Internet.

It is called a distributed system because information can reside on different computers around the world. Yet be easily linked together using hypertext. The web uses hypertext to create links from together using hypertext. The web uses hyperte3xt to create links from one resource to another. A hypertext link is usually displayed by highlighted and underlined text on the page. A hypertext link or hyperlink can also be graphic that acts as a button linking to another resource.

- World Wide Web IS an architectural framework for accessing linked documents called web pages that are spread over thousand of computers all over the world.

WWW is a set of programs, standards and protocols that allow the text, images, animations, sounds and videos to be stored, accessed and linked together in form of web sites.

- The WWW project was developed at CERN, the European Center for Nuclear Research in 1989.

- It has a unique combination of flexibility, portability, and user-friendly features that distinguishes it from the other services provided by the Internet.

Architecture of WWW

- WWW is basically a distributed client-server service. It this, a client can access the services from a server using a browser.

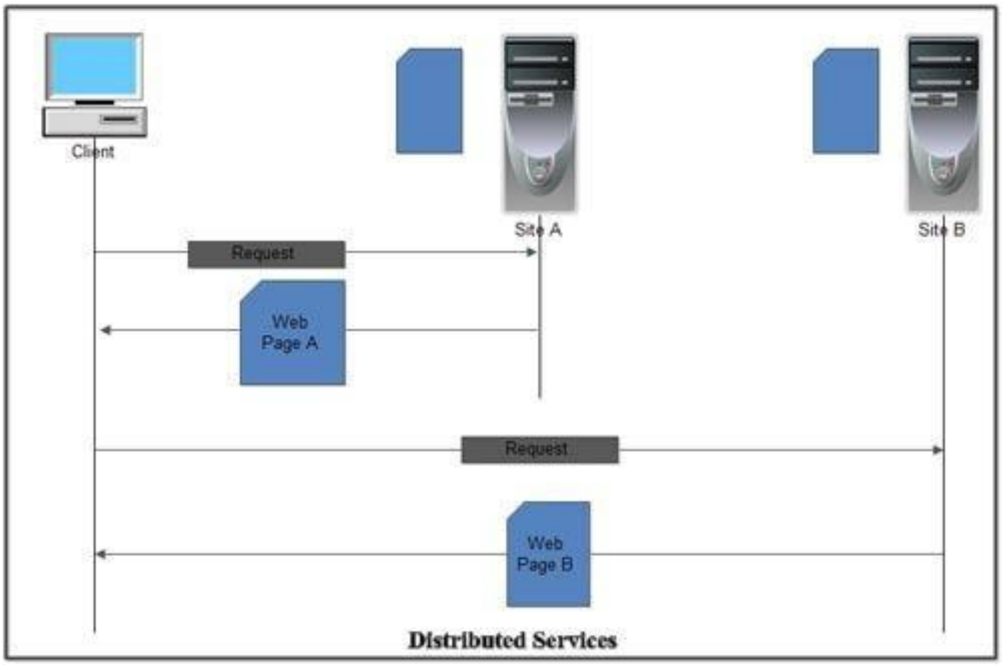
- These services are usually distributed over many locations called sites or websites.

From the user's point of view web consists of a vast worldwide collection of documents called web pages. These web pages reside on different sites or machines all over the world.

- Each web page can contain link to other pages anywhere in the world. By clicking on such link user can access another web page.

- This kind of link can be in form of string of text or picture, sound, movie clip etc.

- Such a text or image that enables the user to link to another web page is called hyperlink.



- The string of text that points to another web page is called hypertext. The difference between the normal text and hypertext is that, when you take the mouse pointer over it, it changes into a hand shaped cursor. Such a text is sometime, underlined and blue is colour.

• Hypermedia is enhanced form of a hyperlink which not only links to the other pages or other sections within the same page but can also link with various medium like sound, animation, movie clip etc, Hypermedia is grouping of different media like sound, graphics, animations and text in a single file.

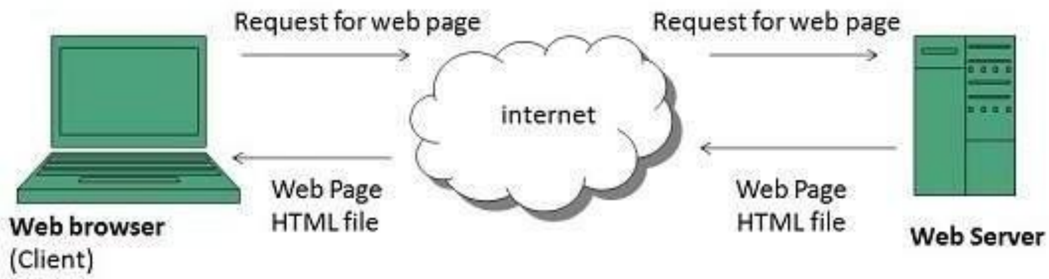
• These hyperlinks are created with the help of specialized language called Hypertext Mark up Language (HTML).

• In order to access these web pages on different sites, each of these pages has a specific address called Uniform Resource Locator (URL).

• Web pages are viewed with a program called a browser.

WWW Operation

1. User enters the URL (say, **http://www.tutorialspoint.com**) of the web page in the address bar of web browser.
2. Then browser requests the Domain Name Server for the IP address corresponding to www.tutorialspoint.com.
3. After receiving IP address, browser sends the request for web page to the web server using HTTP protocol which specifies the way the browser and web server communicates.
4. Then web server receives request using HTTP protocol and checks its search for the requested web page. If found it returns it back to the web browser and close the HTTP connection.
5. Now the web browser receives the web page, It interprets it and display the contents of web page in web browser's window.



Web Documents:

Three basic types of web documents are Static, Dynamic and Active.

Static Web Document:

A static web document resides in a file that it is associated with a web server. The author of a static document determines the contents at the time the document is written. Because the contents do not change, each request for a static document results in exactly the same response.

Dynamic Web Document: A dynamic web document does not exist in a predifined form. When a request arrives the web server runs an application program that creates the document. The server returns the output of the program as a response to the browser that requested the document. Because a fresh document is created for each request, the contents of a dynamic document can vary from one request to another.

Active Web Document: An active web document consists of a computer program that the server sends to the browser and that the browser must run locally. When it runs, the active document program can interact with the user and change the display continously.

Overview of HTTP Protocols:

The Hypertext Transfer Protocol (HTTP) is an application-level protocol for distributed, collaborative, hypermedia information systems. This is the foundation for data communication for the World Wide Web (i.e. internet) since 1990. HTTP is a generic and stateless protocol which can be used for other purposes as well using extensions of its request methods, error codes, and headers.

Basically, HTTP is a TCP/IP based communication protocol, that is used to deliver data (HTML files, image files, query results, etc.) on the World Wide Web. The default port is TCP 80, but other ports can be used as well. It provides a standardized way for computers to communicate with each other. HTTP specification specifies how clients' request data will be constructed and sent to the server, and how the servers respond to these requests.

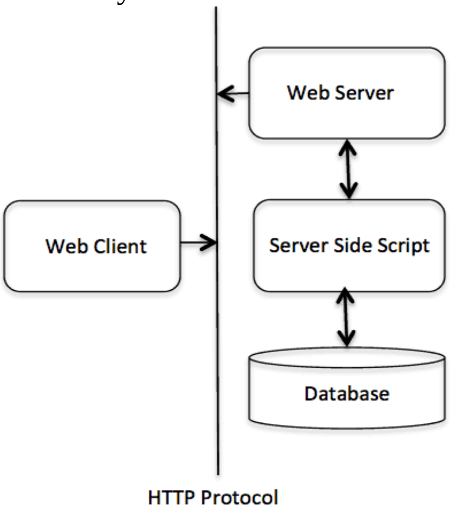
Basic Features

There are three basic features that make HTTP a simple but powerful protocol:

- **HTTP is connectionless:** The HTTP client, i.e., a browser initiates an HTTP request and after a request is made, the client disconnects from the server and waits for a response. The server processes the request and re-establishes the connection with the client to send a response back.
- **HTTP is media independent:** It means, any type of data can be sent by HTTP as long as both the client and the server know how to handle the data content. It is required for the client as well as the server to specify the content type using appropriate MIME-type.
- **HTTP is stateless:** As mentioned above, HTTP is connectionless and it is a direct result of HTTP being a stateless protocol. The server and client are aware of each other only during a current request. Afterwards, both of them forget about each other. Due to this nature of the protocol, neither the client nor the browser can retain information between different requests across the web pages.HTTP/1.0 uses a new connection for each request/response exchange, where as HTTP/1.1 connection may be used for one or more request/response exchanges.

Basic Architecture

The following diagram shows a very basic architecture of a web application.



The HTTP protocol is a request/response protocol based on the client/server based architecture where web browsers, robots and search engines, etc. act like HTTP clients, and the Web server acts as a server.

Client

The HTTP client sends a request to the server in the form of a request method, URI, and protocol version, followed by a MIME-like message containing request modifiers, client information, and possible body content over a TCP/IP connection.

Server

The HTTP server responds with a status line, including the message's protocol version and a success or error code, followed by a MIME-like message containing server information, entity meta information, and possible entity-body content.

KarpagamAcademy of Higher Education
(Established Under Section 3 of UGC Act 1956)
Eachanari Post, Coimbatore – 641 021. INDIA
Phone : 0422-2611146, 2611082 Fax No : 0422 -2611043

Enable | Enlighten | Enrich
(Deemed to be University)
(Under Section 3 of UGC Act 1956)

DEPARTMENT OF COMPUTER APPLICATIONS
BCA (2017-2020 BATCH)

COURSE NAME: COMPUTER NETWORKS **COURSE CODE: 17CAU303**

UNIT V - POSSIBLE QUESTIONS

PART – A (20 Marks)
(Q.No 1 to 20 Online Examinations)

PART – B
(Each question carries two marks)

1. What are the services provided by TCP?
2. Define URL.
3. Define Three Way Handshake.
4. Define TCP.
5. Define WWW.
6. What are the types of web documents?
7. Define DNS.
8. Define HTTP.
9. Define CGI.
10. What are the three phases of connection oriented transmission?

PART –C
(Each question carries six marks)

1. Describe about the flow control in transport layer.
2. Elucidate HTTP with a neat sketch.
3. Explain about error control in transport layer.
4. Explain about Web documents in WWW.
5. Explain the connection establishment in TCP.
6. Explain the DNS protocol
7. Explain the architecture of World Wide Web with neat sketch.
8. Explain the TCP Services.
9. Explain the HTTP Protocol
10. Explain the User Datagram Protocol.

Karpagam Academy of Higher Education

Department of Computer Applications

BCA (2017-2020 Batch)

COMPUTER NETWORKS (17CAU303)

UNIT- V

S.No	Question	Option1	Option2	Option3	Option4	Answer
1	TCP is responsible for __________ delivery	hop-to-hop	process-to-process	host-to-host	node-to-node	process-to-process
2	FTP stands for _________	File Transmission Protocol	File Transfer Protocol	File Translation Protocol	File Transition Protocol	File Transfer Protocol
3	TELNET stands for ________	Transfer Network	Transfer Node	Terminal Network	Terminal Node	Terminal Network
4	______ is the Port number for Terminal Network	20	21	23	25	23
5	RPC stands for _______	Random Procedure Call	Remote Procedure Call	Rapid Procedure Call	Reverse Procedure Call	
6	_______ is the port number for Remote Procedure Call	111	7	9	79	111
7	HTTP stands for _______	Hyper Text Transfer Protocol	Hyper Text Transmission	Hyper Text Transition Protocol	Hyper Text Translation Protocol	Hyper Text Transfer Protocol
8	______ is the Port number for HTTP.	7	9	79	80	80
9	TCP transmits data in _______ mode	duplex	simplex	full duplex	half duplex	full duplex
10	In TCP, one end can stop sending data while still receiving data called _______	active open	passive open	half close	full close	half close
11	RTO stands for ______	Retransmission Time Out	Repair Time Out	Repeat Time Out	Retransfer Time Out	Retransmission Time Out
12	RTT stands for ______	Round Trip Time	Round Transfer Time	Rapid Trip Time	Rotational Trip Time	Round Trip Time
13	The opened, closed and shrunk activities of a window is controlled by ______	sender	receiver	transmitter	controller	**receiver**
14	The window size is determined by ______	maximum(rwnd, cwnd)	maximum(swnd, cwnd)	minimum(swnd, cwnd)	minimum(rwnd, cwnd)	minimum(rwnd, cwnd)
15	Which of the tool is not included for error detection and correction in TCP?	checksum	acknowledgement	flag	time-out	flag
16	If more than one station tries to send, there is conflict called ____	congestion	collision	contention	traffic	collision
17	The value of RTO is dynamic in TCP and is updated based on _______segment.	RTO	RTT	ACK	none	RTT

18	An ACK segment,if carrying ________data consumes no sequence number.	no	2	3	5	no
19	SCTP stands for ______	String Control Transmission Protocol	Stream Control Transmission	Stack Control Transmission Protocol	Signal Control Transmission Protocol	Stream Control Transmission Protocol
20	TCP is ___________ protocol	message oriented	byte oriented	bit oriented	text oriented	byte oriented
21	UDP is ___________ protocol	message oriented	byte oriented	bit oriented	text oriented	message oriented
22	_________ is a protocol combines the best features of TCP and UDP	SCTP	SNMP	SMTP	FTP	SCTP
23	WWW stands for ________	Web Wide World	World Wide Web	Wide World Web	World Wise Web	World Wide Web
24	SMTP stands for _______	Simple Mail Transfer Protocol	Simple Message Transfer Protocol	Single Mail Transfer Protocol	Single Message Transfer Protocol	Simple Mail Transfer Protocol
25	_______ is a supporting program that is used by other programs such as email.	HTTP	DNS	FTP	SMTP	DNS
26	DNS stands for _______	Domain Name Source	Domain Name Service	Domain Name System	Domain Name Sender	Domain Name System
27	In a _______ name space, a name is assigned to an address.	Flat	Hierarchical	Fully Qualified	Partially Qualified	Flat
28	In a _______ name space, ech name is made of several parts	Flat	Hierarchical	Fully Qualified	Partially Qualified	Hierarchical
29	If a label is terminated by a null string, it is called ________ name space	Flat	Hierarchical	Fully Qualified	Partially Qualified	Fully Qualified
30	If a label is not terminated by a null string, it is called ________ name space	Flat	Hierarchical	Fully Qualified	Partially Qualified	Partially Qualified
31	A full domain name is sequence of labels seperated by ______	colons	Semicolons	dots	commas	dots
32	URL stands for ______	Uniform Resource Location	Uniform Resource Locator	Uniform Remote Location	Uniform Remote Locator	Uniform Resource Locator
33	The URL defines ________ things.	two	three	four	five	four
34	The ________ is the client/server program used to retrieve the document.	protocol	host	port	path	protocol
35	The ________ is the computer on which the inforation is located.	protocol	host	port	path	host
36	The documents in WWW can be grouped into _______ categories	two	three	four	five	three
37	_________ is fixed content document that is created and stored in a server	static document	dynamic document	active document	passive document	static document
38	_________ is created by a web server whenever the browser requests the document	static document	dynamic document	active document	passive document	dynamic document
39	For many applications, a program or script to be run at the client side is called _______	static document	dynamic document	active document	passive document	active document
40	_________ is a language is used for creating web page.	Pascal	C	C++	HTML	HTML

41	HTML stands for______	Hyper Text Markup Language	Hyper Text Model Language	Hyper Transmission Markup Language	Hyper Transmission Model Language	Hyper Text Markup Language
42	CGI stands for ________	Computer Gateway Interface	Common Gateway Interface	Computer Gateway Information	Common Gateway Information	Common Gateway Interface
43	Which of the following tag is used for underline the text	<L>…..</L>	<UL>…..</UL>	<U>…..</U>	<I>…..</I>	<U>…..</U>
44	________ documents are sometimes referred to as server site dynamic documents.	static documents	dynamic documents	active documents	passive documents	dynamic documents
45	Which of the following tag is used to make the text Italic	<L>…..</L>	<B>…..</B>	<U>…..</U>	<I>…..</I>	<I>…..</I>
46	HTTP is a ________ protocol.	application layer	presentation layer	physical layer	transport layer	application layer
47	In the network HTTP resources are located by	unique resource locator	uniform resource identifier	unique resource identifier	uniform resource locator	uniform resource identifier
48	HTTP client requests by establishing a __________ connection to a particular port on the server.	user datagram protocol	transmission control protocol	broader gateway protocol	Internet Protocol	transmission control protocol
49	FTP server listens for connection on port number	20	21	23	25	21
50	The communication protocol used by Internet is ________	FTP	TELNET	HTTP	TCP/IP	TCP/IP

Reg No. ………………..
[17CAU303]

Karpagam Academy of Higher Education

(Established Under Section 3 of UGC Act 1956)

COIMBATORE – 641 021

BCA Degree Examination

(For the candidates admitted from 2017 onwards)

Third Semester

First Internal Exam July 2018

COMPUTER NETWORKS

Duration: 2 Hrs **Maximum Marks: 50 Marks**
Date & Session: **Class: II BCA**

Part - A (20 X 1 = 20 Marks)
(Answer all the Questions)

1. _____________is a set of devices connected by a communication links.
 a. Protocol b. Topology **c. Network** d. Satellite

2. Any device that connected to a network is called as _________
 a. client b. server **c. node** d. link

3. There are________layers in ISO OSI model.
 a. 4 b. 5 c. 6 **d. 7**

4. The term________refers to the way in which a network is laid physically
 a. protocol **b. topology** c. network d. satellite

5. In a Star topology, each device has a dedicated point to point link only to a central controller called a ___________
 a. hub b. repeater c. router d. controller

6. OSI stands for_______
 a. Open Systems Interconnection b. Open Standard Interconnection
 c. Open Systems Interface d. Open Standard Interface

7. In_________topology one long cable acts as a backbone to link all the devices in a network.
 a. star **b. bus** c. mesh d. ring

8. _________size is limited to few kilometers
 a. MAN b. WAN **c. LAN** d. Internet

9. ATM stands for _________
 a. Asynchronous Transmission Mode **b. Asynchronous Transfer Mode**
 c. Asynchronous Transmission Medium d. Asynchronous Transfer Medium

10. A________connection provides a dedicated link between two devices
 a. point-to-point b. multi-point c. physical d. logical

11. _________is a set of rules.
 a. Protocol b. Topology c. Network d. Satellite

12. The______layer is concerned with the syntax and semantics of the information exchanged between two systems.
 a. application **b. presentation** c. session d. physical

13. The completion of one full pattern is called ______
 a. period b. signal c. wave **d. cycle**

14. UDP stands for ________
 a. Uniform Datagram Protocol **b. User Datagram Protocol**
 c. Uniform Datagram Packet d. User Datagram Packet

15. __________is used to facilitate simultaneous transmission of a message to a group of recipient.
 a. ARP b. RARP c. ICMP **d. IGMP**

16. NIC stands for _________

a. Network Interface Connection **b. Network Interface Card**
c. Network Interface Communication d. Network Interface Control

17. Period and Frequency is calculated by _______

a. F=1/t and T=1/f b. F=f/t and T=t/f c. C=t/f d. T=c/f

18. _____is the process of converting digital to digital signals.

a. line decoding b. block coding **c. line encoding** d. block encoding

19. ______is the set of techniques that allows the simultaneous transmission of multiple signals across a single data link.

a. multiplexing b. demultiplexing c. Spreading d. Transferring

20. TDM stands for __________

a. Time Division Multiplexing b. Transmission Division Multiplexing
c. Time Direction Multiplexing d. Transmission Direction Multiplexing

Part - B (3 X 2=6 Marks)
(Answer all the Questions)

21. What is Network?

Answer:

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

22. Define LAN.

Answer:

A computer network spanned inside a building and operated under single administrative system is generally termed as **Local Area Network (LAN).** Usually, LAN covers an organization' offices, schools, colleges or universities.

23. What are the key elements of a protocol?

Answer:

• Key elements of a protocol:

—**Syntax**

• Structure or format of data, meaning the order in which they are presented

—**Semantics**

• Refer to the meaning of each section of bits, how a particular pattern is interpreted and what action to be taken

—**Timing**

• Refers to when data should be sent and how fast can they be sent

Part - B (3 X 8 =24 Marks)
(Answer all the Questions)

24. (a) Explain the types of Topology.
Answer:

Network Topologies:

The arrangement of a network which comprises of nodes and connecting lines via sender and receiver is referred as network topology. The various network topologies are:

a) Mesh Topology:

In mesh topology, every device is connected to another device via particular channel.

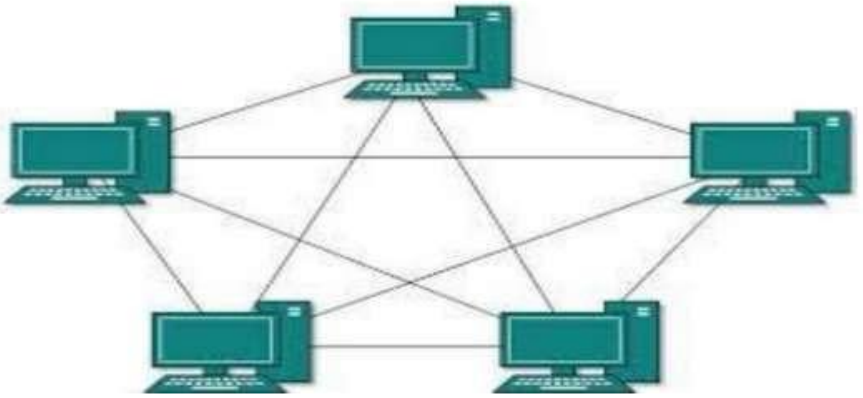


Figure 1 : Every device is connected with another via dedicated channels. These channels are known as links.

- If suppose, N number of devices are connected with each other in mesh topology, then total number of ports that is required by each device is N-1. In the Figure 1, there are 5 devices connected to each other, hence total number of ports required is 4.

- If suppose, N number of devices are connected with each other in mesh topology, then total number of dedicated links required to connect them is $^{N}C_{2}$ i.e. N(N-1)/2. In the Figure 1, there are 5 devices connected to each other, hence total number of links required is 5*4/2 = 10.

b) Star Topology:

- In star topology, all the devices are connected to a single hub through a cable.
- This hub is the central node and all others nodes are connected to the central node.
- The hub can be passive in nature i.e. not intelligent hub such as broadcasting devices,
- The hub can be intelligent known as active hubs.
- Active hubs have repeaters in them.

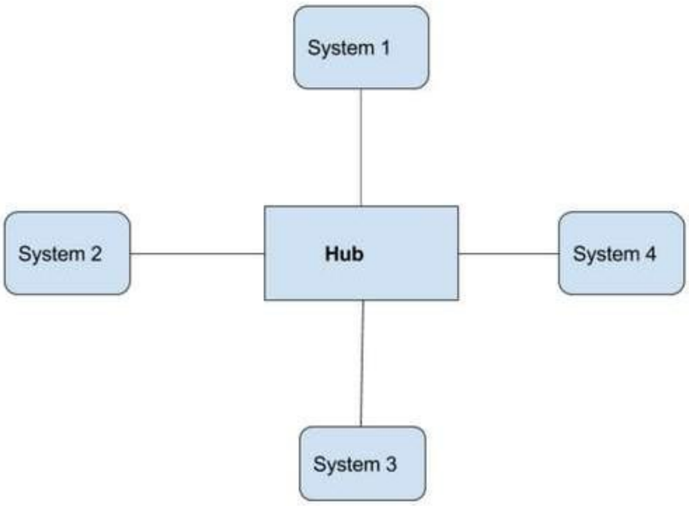


Figure 2: A star topology having four systems connected to single point of connection i.e. hub.

c) Bus Topology:

- Bus topology is a network type in which every computer and network device is connected to single cable.
  It transmits the data from one end to another in single direction.
- No bi-directional feature is in bus topology.

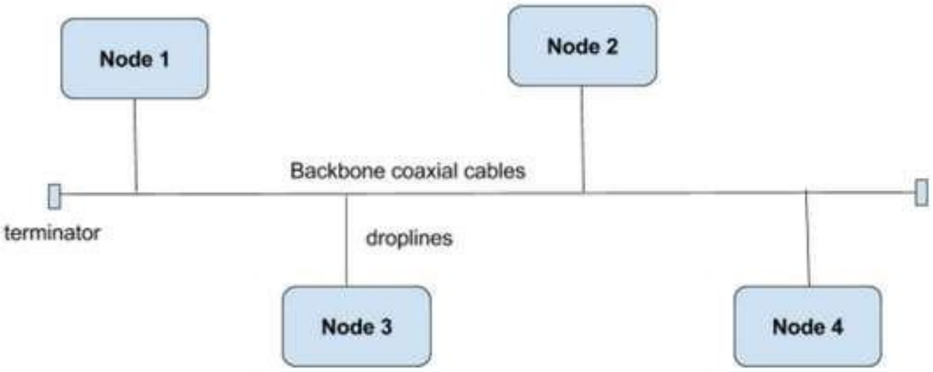


Figure 3: A bus topology with shared backbone cable. The nodes are connected to the channel via drop lines.

d) Ring Topology:

In this topology, it forms a ring connecting a devices with its exactly two neighbouring devices.

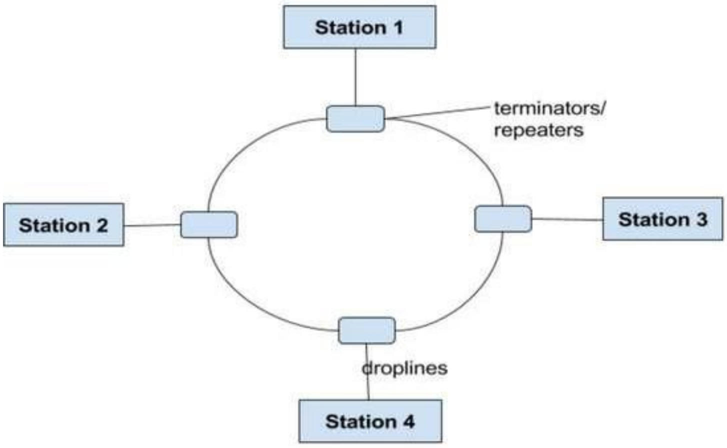


Figure 4 : A ring topology comprises of 4 stations connected with each forming a ring..

e) Hybrid Topology:

This topology is a collection of two or more topologies which are described above. This is a scalable topology which can be expanded easily. It is reliable one but at the same it is a costly topology.

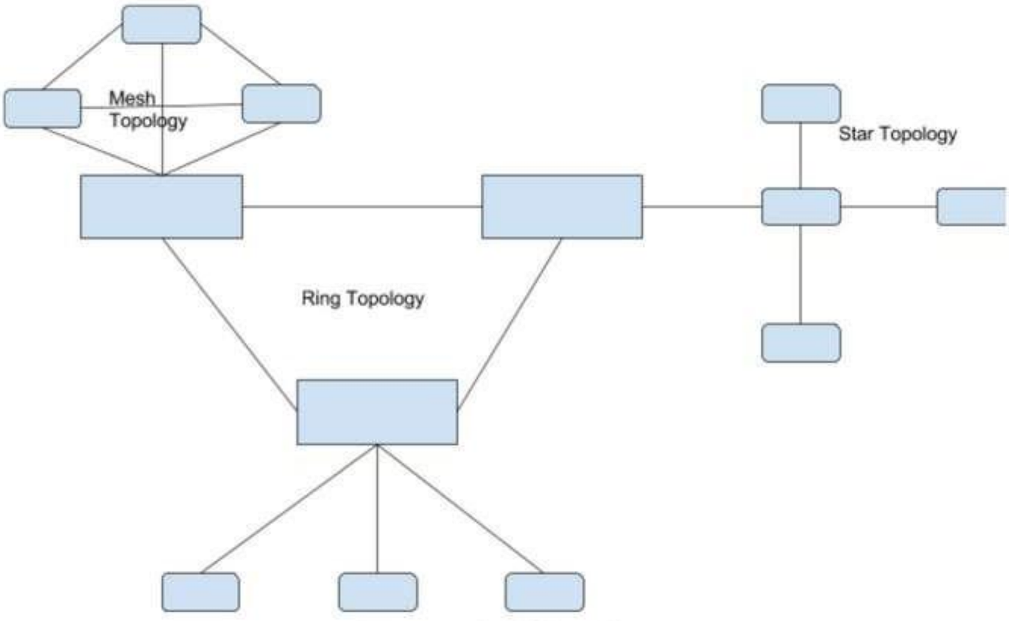


Figure 5 : A hybrid topology

Figure 5: A hybrid topology which is a combination of ring and star topology.

(OR)

(b) What are the categories of networks?

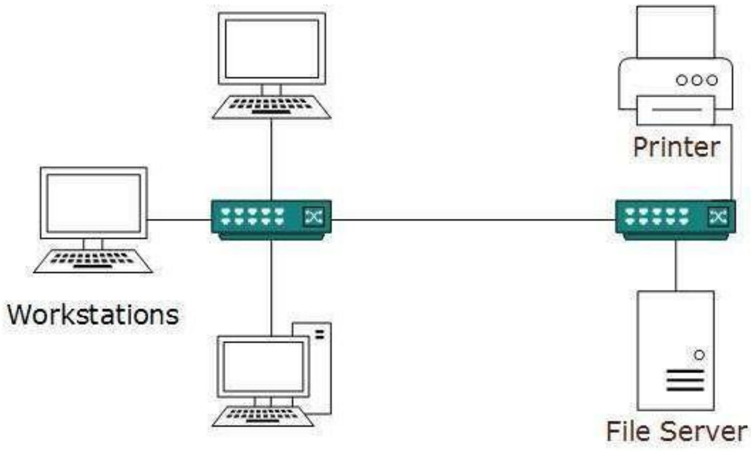
Answer:

Network Categories:

Local Area Network:

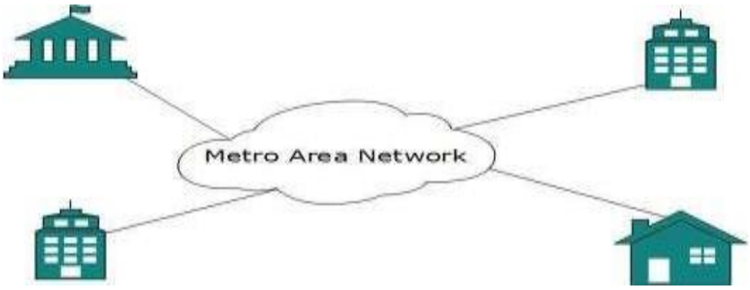
- A computer network spanned inside a building and operated under single administrative system is generally termed as Local Area Network (LAN).
- Usually, LAN covers an organization' offices, schools, colleges or universities.

- Number of systems connected in LAN may vary from 2 to 16 million.
- LAN provides a useful way of sharing the resources between end users.
- The resources such as printers, file servers, scanners, and internet are easily sharable among computers.
- It may contain local servers serving file storage and other locally shared applications.
- It mostly operates on private IP addresses and does not involve heavy routing.
- LAN uses either Ethernet or Token-ring technology.
- LAN can be wired, wireless, or in both forms at once.



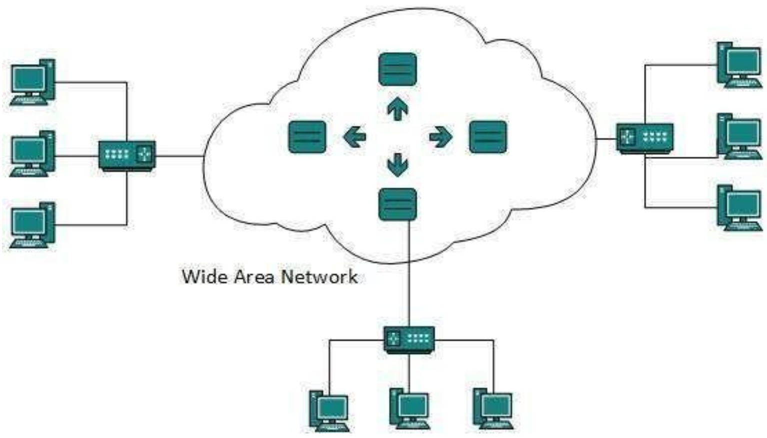
Metropolitan Area Network:

- The Metropolitan Area Network (MAN) generally expands throughout a city such as cable TV network.
- It can be in the form of Ethernet, Token-ring, ATM, or Fiber Distributed Data Interface (FDDI).
- Metro Ethernet is a service which is provided by ISPs.
- This service enables its users to expand their Local Area Networks.
- MAN can help an organization to connect all of its offices in a city.
- Backbone of MAN is high-capacity and high-speed fiber optics.
- MAN works in between Local Area Network and Wide Area Network.



Wide Area Network:

- Wide Area Network (WAN) covers a wide area which may span across provinces and even a whole country.
- Generally, telecommunication networks are Wide Area Network.
- These networks provide connectivity to MANs and LANs.
- WANs are equipped with very high speed backbone,
- WANs use very expensive network equipment.



Internetwork:

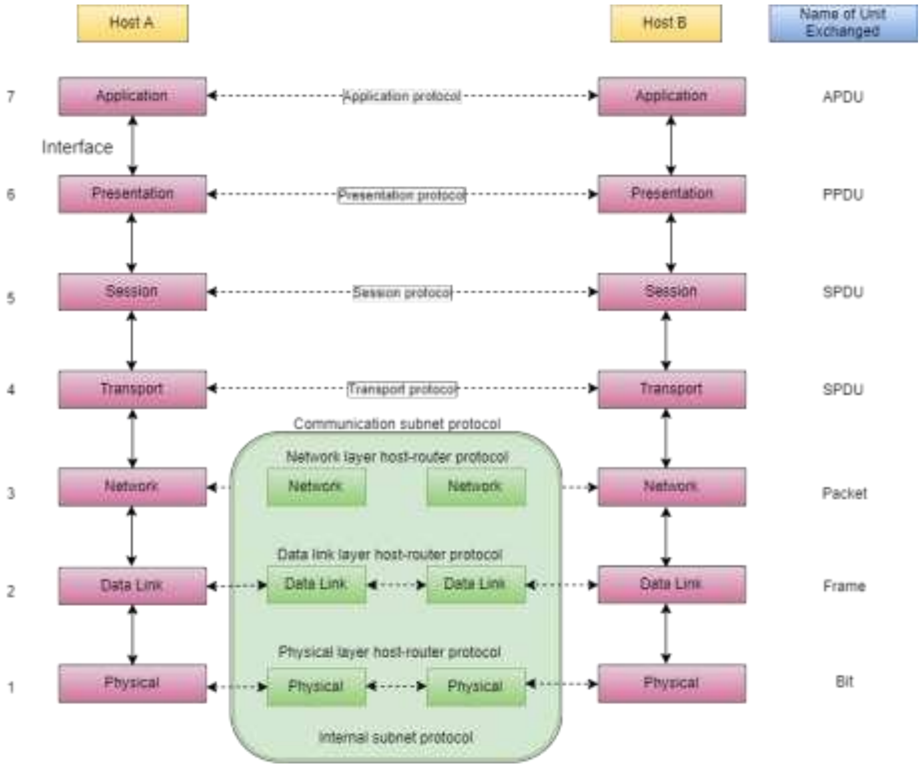
- A network of networks is called an internetwork, or simply the internet.
- It is the largest network in existence on this planet.
- The internet hugely connects all WANs and it can have connection to LANs and Home networks.
- Internet uses TCP/IP protocol suite and uses IP as its addressing protocol.
- Internet is widely implemented using IPv4.
- Internet enables its users to share and access enormous amount of information worldwide.

25. (a) Explain the ISO OSI model with neat sketch.

Answer:

ISO OSI Model:

OSI stands for **Open Systems Interconnection**. It has been developed by ISO – **International Organization of Standardization**‘, in the year 1974. The ISO-OSI model is a seven layer architecture.



The Physical Layer: (Layer 1)

1. It is the lowest layer of the OSI Model.
2. It activates, maintains and deactivates the physical connection.
3. It is responsible for transmission and reception of the unstructured raw data over network.
4. Voltages and data rates needed for transmission is defined in the physical layer.
5. It converts the digital/analog bits into electrical signal or optical signals.
6. Data encoding is also done in this layer.
7. The functions of this layer are Physical characteristics of interfaces and media, Representation of bits, Data rate, Synchronization of bits, Line configuration, Physical topology and Transmission mode.

Data Link Layer: (Layer 2)

1. Data link layer synchronizes the information which is to be transmitted over the physical layer.
2. The main function of this layer is to make sure data transfer is error free from one node to another, over the physical layer.
3. Transmitting and receiving data frames sequentially is managed by this layer.
4. This layer sends and expects acknowledgements for frames received and sent respectively. Resending of non-acknowledgement received frames is also handled by this layer.
5. This layer establishes a logical layer between two nodes and also manages the Frame traffic control over the network. It signals the transmitting node to stop, when the frame buffers are full.
6. The functions of this layer are Framing, Physical addressing, Flow control, Error control and Access control

The Network Layer: (Layer 3)

1. It routes the signal through different channels from one node to other.
2. It acts as a network controller. It manages the Subnet traffic.
3. It decides by which route data should take.
4. It divides the outgoing messages into packets and assembles the incoming packets into messages for higher levels.
5. The functions of this layer are Logical addressing and Routing

The Transport Layer: (Layer 4)

1. It decides if data transmission should be on parallel path or single path.
2. Functions such as Multiplexing, Segmenting or Splitting on the data are done by this layer
3. It receives messages from the Session layer above it, converts the message into smaller units and passes it on to the Network layer.
4. Transport layer can be very complex, depending upon the network requirements.
5. Transport layer breaks the message (data) into small units so that they are handled more efficiently by the network layer.
6. The functions of the Transport layer are Service-point (port) addressing, Segmentation and reassembly, Connection control, Flow control and Error control

The Session Layer: (Layer 5)

1. Session layer manages and synchronize the conversation between two different applications.
2. Transfer of data from source to destination session layer streams of data are marked and are resynchronized properly, so that the ends of the messages are not cut prematurely and data loss is avoided.
3. The functions of this layer are Session establishment, maintenance and termination, Synchronization and Dialog Controller

The Presentation Layer: (Layer 6)

1. Presentation layer takes care that the data is sent in such a way that the receiver will understand the information (data) and will be able to use the data.
2. While receiving the data, presentation layer transforms the data to be ready for the application layer.
3. Languages (syntax) can be different of the two communicating systems. Under this condition presentation layer plays a role of translator.
4. The functions of the Presentation layer are Translation, Encryption/ Decryption and Compression

Application Layer: (Layer 7)

1. It is the topmost layer.
2. This layer mainly holds application programs to act upon the received and to be sent data.
3. The functions of this layer are Network Virtual Terminal, FTAM-File transfer access and management, Mail Services and Directory Services.

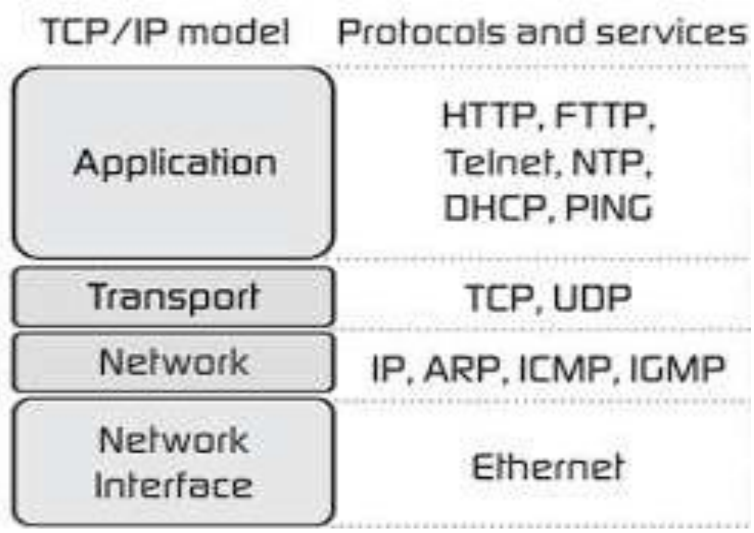
(OR)

(b) Discuss the TCP/IP Protocol Suite.

Answer:

TCP/IP Protocol Suite:

The **TCP/IP model** is a concise version of the OSI model. It contains four layers, unlike seven layers in the OSI model. :



Network Interface Layer:

1. It is also called as Host-to-network layer.
2. Lowest layer of the all.
3. Protocol is used to connect to the host, so that the packets can be sent over it.
4. Varies from host to host and network to network.

Internet layer:

1. Selection of a packet switching network which is based on a connectionless internetwork layer is called a internet layer.
2. It is the layer which holds the whole architecture together.
3. It helps the packet to travel independently to the destination.
4. Order in which packets are received is different from the way they are sent.
5. The main protocols residing at this layer are :
   - **IP (Internet Protocol)**
   - **ICMP (**Internet Control Message Protocol)
   - **ARP (**Address Resolution Protocol)

Transport Layer:

1. It decides if data transmission should be on parallel path or single path.
2. Functions such as multiplexing, segmenting or splitting on the data is done by transport layer.
3. The applications can read and write to the transport layer.
4. Transport layer adds header information to the data.
5. Transport layer breaks the message (data) into small units so that they are handled more efficiently by the network layer.
6. Transport layer also arrange the packets to be sent, in sequence.
7. The two main protocols present in this layer are:
   - **Transmission Control Protocol (TCP)**
   - **User Datagram Protocol (UDP)**

Application Layer:

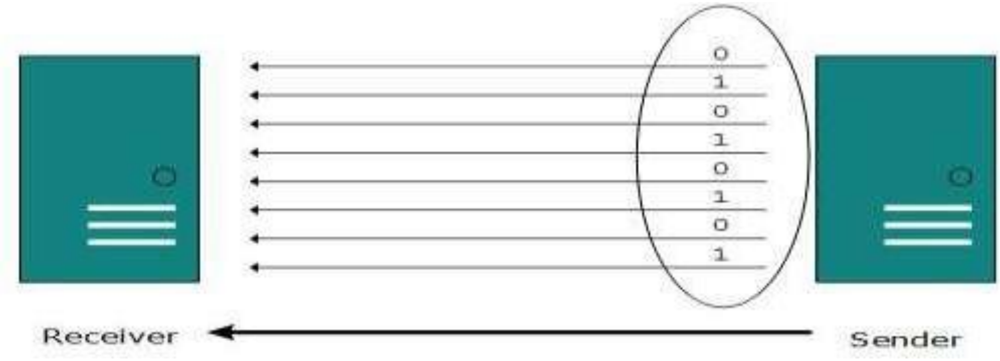
The TCP/IP specifications described a lot of applications that were at the top of the protocol stack. Some of them were TELNET, FTP, SMTP, DNS etc.

1. TELNET is a two-way communication protocol which allows connecting to a remote machine and run applications on it.
2. FTP (File Transfer Protocol) is a protocol, that allows File transfer amongst computer users connected over a network. It is reliable, simple and efficient.
3. SMTP (Simple Mail Transport Protocol) is a protocol, which is used to transport electronic mail between a source and destination, directed via a route.
4. DNS (Domain Name Server) resolves an IP address into a textual address for Hosts connected over a network.

26. (a) Explain about the parallel transmission.
Answer:

Parallel Transmission:

- The binary bits are organized in-to groups of fixed length.
- Both sender and receiver are connected in parallel with the equal number of data lines.
- Both computers distinguish between high order and low order data lines.
- The sender sends all the bits at once on all lines.
- The data lines are equal to the number of bits in a group or data frame, a complete group of bits (data frame) is sent in one go.
- Advantage of Parallel transmission is high speed
- Disadvantage is the cost of wires, as it is equal to the number of bits sent in parallel.

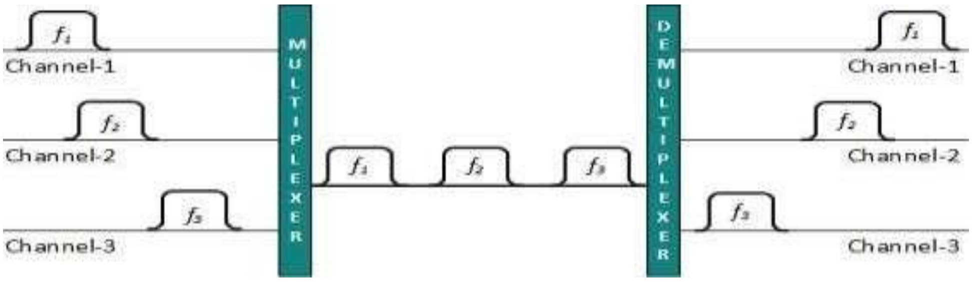


(OR)

(b) Explain the Time Division Multiplexing.
Answer:

Frequency Division Multiplexing (FDM):

- When the carrier is frequency, FDM is used.
- FDM is an analog technology.
- FDM divides the spectrum or carrier bandwidth in logical channels and allocates one user to each channel.
- Each user can use the channel frequency independently and has exclusive access of it.
- All channels are divided in such a way that they do not overlap with each other.
- Channels are separated by guard bands.
- Guard band is a frequency which is not used by either channel.


f_1
Channel-1
f_2
Channel-2
f_3
Channel-3
MULTIPLEXER
f_1
f_2
f_3
DEMULTIPLEXER
f_1
Channel-1
f_2
Channel-2
f_3
Channel-3