Course Title : Computer Networks
Course no : CSC-301
Credit hours : 3

Full Marks : 60+20+20
Pass Marks : 24+8+8

Course Contents:

Unit 1. -35 Hrs.

1.1 Computer Network: Introduction to networking, computer network, Internet, the network edge: end system, clients, server, connection oriented and connectionless service, network core, network access and physical media, ISPs and back bone.

1.2 Protocol Layers: Introduction, layered architecture, The Internet protocol stack, network entities and layers.

1.3 Application Layer: Introduction, principles of application layer protocols, the web and HTTP, file transfer, Domain Name service (DNS): Working of DNS, DNS records, DNS messages.

1.4 Transport Layer: Introduction, relationship between transport layer and network layer, transport layer in the Internet, multiplexing and demultiplexing, connectionless transport, reliable data transfer: Building a reliable data transfer protocol, pipelined reliable data transfer protocol, Go-Back-N (GBN), selective repeat (SR), connection oriented transport: TCP, TCP connection, TCP segment structure, time estimation and time out, flow control, Principle of congestion control: The causes and costs of congestion, approaches to congestion control,

1.5 Network Layer : Introduction, network service model, datagrams and virtual circuit service, routing principles: A link state routing algorithm, the distance vector routing algorithm, hierarchical routing, The Internet protocol (IP) : IPV4 addressing, datagram format, IP datagram fragmentation, Internet Control Message Protocol [ICMP], Network address translator, routing in the Internet, IPV6, Multicasting routing.

Unit 2 -12 Hrs.

2.1 Link Layer and Local Area Networks: Introduction, Data link layer: the services provided by the link layer, error detection and error correction techniques, multiple access protocols, LAN addresses and Address Resolution Protocol, Ethernet, Wireless Links: IEEE 802.11b, Bluetooth, Point to point protocol (PPP), Asynchronous Transfer Mode (ATM), frame relay.

2.2 Multimedia Networking: Introduction, multimedia networking application, steaming audio and video.

2.3 Network Management: Introduction, The infrastructure for network management

Text books: Computer Networking; A Top Down Approach Featuring The Internet, 2nd Edition.

Computer Network

Introduction:

The network consist of two or more than two computer or computer devices connected together for the purpose of communication or data storing.

Why networking?

i) Information sharing
ii) Sharing hardware or software

Type of Computer Network

1. Based on transmission media
   co-axial cable, optical fiber

2. Based on transmission area
   LAN, MAN, WAN

3.

i) Based on management method
   a. Peer to Peer
   b. Client Server

ii) Based on topology

Difference between LAN, MAN and WAN

a. **Local Area Network (LAN):**

A network that connects a group of computer in a small geographical area. Ownership type of LAN is private. Design and maintenance is easy. Propagation delay is short. High speed. It is mainly used in college, school and hospital.

b. **Metropolitan Area Network (MAN):**

It covers relatively large region such as city, towns, Ownership type: private or public. Design and maintenance: difficult. Propagation delay: moderate. Used for small town, city, etc.

c. **Wide Area Network (WAN):**

It spans large locality and connects countries together. Ownership type: private or public. Design and maintenance: difficult. Propagation delay: long. Speed: low. Used for countries and continent.

Unit 1

Computer Network :-

Computer Network is a communication network which allows node to share resources. In computer networks, computing devices exchange data with each other using connections between nodes. These data links are established over cable media such as wires or optical fibers or wireless media such as Wi-Fi. Network device that originates, route and terminate the data are called network nodes. Nodes can include host such as personal computers, phones, servers as well as networking hardwares like switch, hub, routers. Two such devices can be said to be networked together when one or both of them is able to exchange information with each other. Computer network supports an enormous number of applications and services such as access to world wide web, audio/video transmission, shared use of application and storage servers, printers, fax machines, and use of email, instant messaging application.

Computer Network differs in the transmission medium used to carry their signals, communication protocols to organize network traffic, the network size, topology, traffic control mechanism and organizational structure.

The best known computer network is the 'Internet'.

Transmission mode in Computer Network:

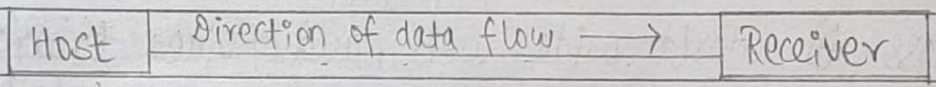
Transmission mode means transferring of data between two devices. It is also called communication mode. These modes detect the direction of flow of information. There are three types of transmission modes:

i) Simplex mode
ii) Half duplex mode
iii) Full duplex mode

i) Simplex mode:

In this type of transmission mode, data can be sent only through one direction i.e. communication is unidirectional. We cannot send a message back to the sender.

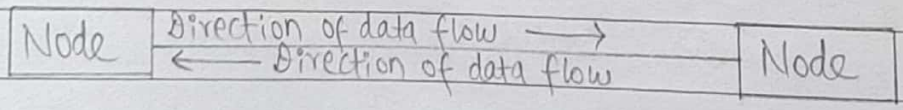
Example: Loudspeaker, TV broadcasting, radio broadcasting, etc.



ii) Half duplex mode:

In half duplex system, we can send data in both directions but it is done one at a time i.e. when a sender is sending a data then at that time we cannot send our message to the sender.

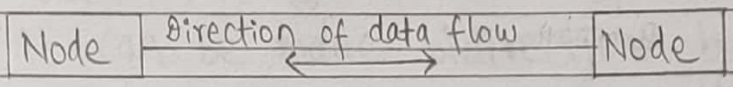
Example: Walkie-Talkie.



iii) Full duplex mode:

In full duplex system, we can send data in both directions as it is ~~direct~~ bi-directional. Data can be sent both direction simultaneously.

Example: Telephone



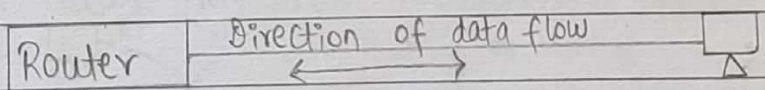
Network Topology:-

Network topology is the representation of networks arrangement, connecting various nodes through lines of connection.

Types of network topology are:-

1) Point to Point (P to P):

Point to point network contains exactly two nodes that may be computers, switches or routers. The receiving end of one node is connected to sending end of other node and vice-versa.



ii) Bus topology:

Bus topology uses one cable to connect multiple computers. The cable is also called trunk or segment. T-shaped like connectors named as T-connectors are used to connect the cable segment. Co-axial cable are used as connection medium in bus topology. Only one computer at a time can transmit data on a bus topology. Computers in bus topology listens to all traffic on the network but accept only those data that are addressed to them. Broadcast packets are an exception because all computers on the network accept them.

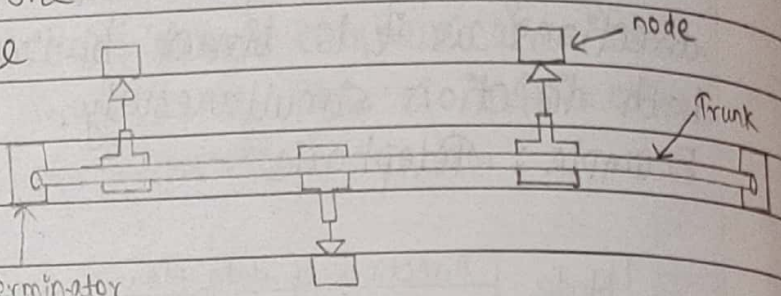


Fig: Bus Topology

Advantages:
i) Cost effective
ii) Bus topology uses less cable

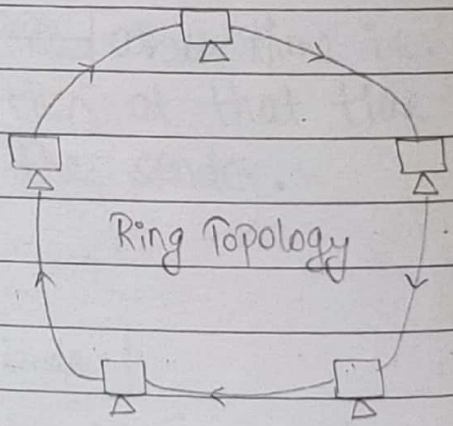
Disadvantages:
i) Bus topology is outdated.
ii) Collision occurs if two PCs try to send data simultaneously.

Terminator:-

Terminator are the resistors that are connected to each end of the trunk. These resistors are used to neutralize all garbage data of the trunk cable.

iii) Ring Topology:

It is called ring topology because it forms a ring as each computer is connected to another computer with the last one connected to the first. Exactly two neighbours for each device.



Advantages:
i) Transmitting network is not affected by high traffic as only one node have token to transmit data.

Disadvantages: i) Adding and deleting the computer disturbs the network activities.
ii) Failure in one computer disturbs the whole network.

A number of repeaters are used for ring topology with large number of nodes because if someone wants to send some data to the last node in the ring topology with 100 nodes then the data will have to pass through 99 nodes to reach the 100th nodes. Hence, to prevent data loss, repeaters are used in the network. The transmission is unidirectional but it can be made bidirectional by having two connections between each node, it is called dual ring topology which can also be used as backup if one ring connection is broken.

iv) Daisy chain:

This topology connects all the nodes in a linear fashion. Similar to ring topology, all nodes are connected to two nodes only except the end nodes.

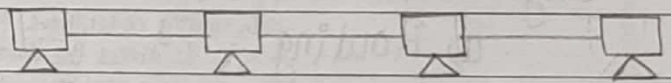


Fig: Daisy chain

Means if the end node in daisy chain are connected then it represents ring topology. Link failure in this topology splits the network into two segment. Every intermediate nodes work as relay for its immediate node.

v) Star topology:

In this type of topology, all the computers are connected to a single switch through a cable. This switch is a central node and all other nodes are connected to the central node.

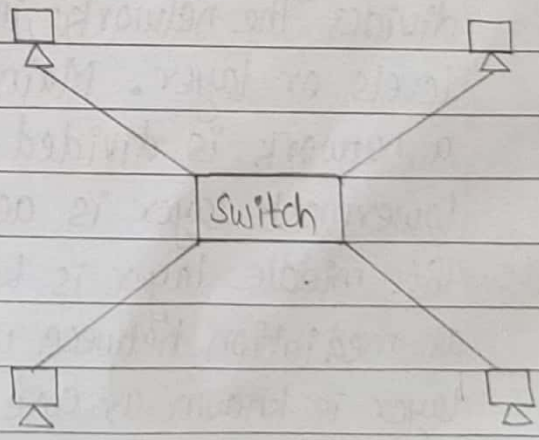


Fig: Star topology

Star Topology:

Advantages: i) Fast performance with few nodes and low network traffic.
ii) Only the node is affected which has failed, rest of node can work smoothly.

Disadvantages: i) Cost of installation is high.
ii) Performance is based on hub.
iii) If the hub fail then the whole network is stopped because all the node depend on the hub.

Every node in the star topology has its own dedicated connections to the switch. Switch also act as a repeater for data flow.

VI) Mesh Topology:

It is a point-to-point connection to other nodes or devices. Mesh has $n(n-1)/2$ physical channels to link n-devices. There are two techniques to transmit data over the mesh topology, they are:

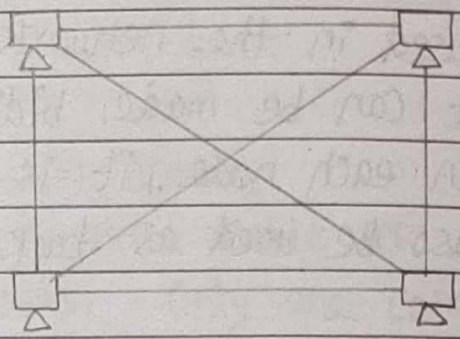


Fig: Mesh Topology

a) Routing ⇒ In routing nodes have routing logic as per the network requirements. Like routing logic to direct the data to reach the destination using the shortest distance.
b) Flooding ⇒ In flooding, the same data is transmitted to all the nodes hence no routing logic is required but it leads to unwanted load over the network.

VII) Tree Topology:

Tree topology is also known as hierarchical topology, this is most common form of topology used. This topology divides the network into multiple levels or layer. Mainly in LANs a network is divided into three type of network devices. The lowermost layer is access layer where computers are attached. The middle layer is known as distribution layer which work as mediation between upper layer and lower layer. The highest layer is known as core layer and is the central point of the

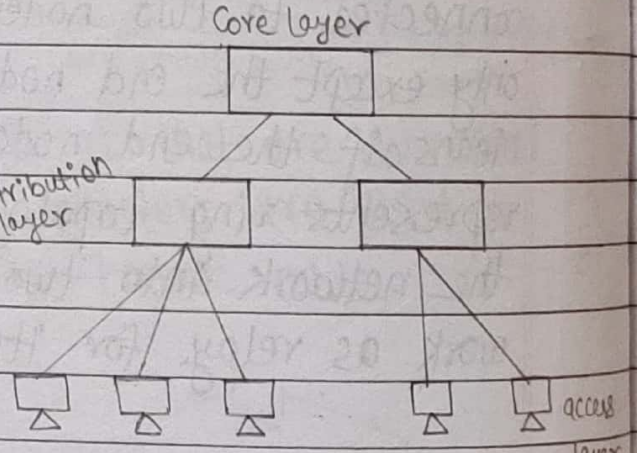


Fig: Tree Topology

Mesh Topology:

Advantages: i) Fault tolerance i.e. if there is a break in a cable segment, traffic can be re-routed. This fault tolerance means that the network going down due to a cable, fault is almost impossible.

Disadvantages: i) A mesh topology is a very hard to administrator and manage because of the numerous connections.
ii) It is costly with large network, the amount of cable needed is large.

network i.e. root of the tree from which all nodes fork.

viii) Hybrid Topology:

The combination of two or more than two types of other topologies is commonly known as hybrid topology. For example: In an office, in one department, ring topology is used and in another star topology is used, connecting these topologies will result in hybrid topology.

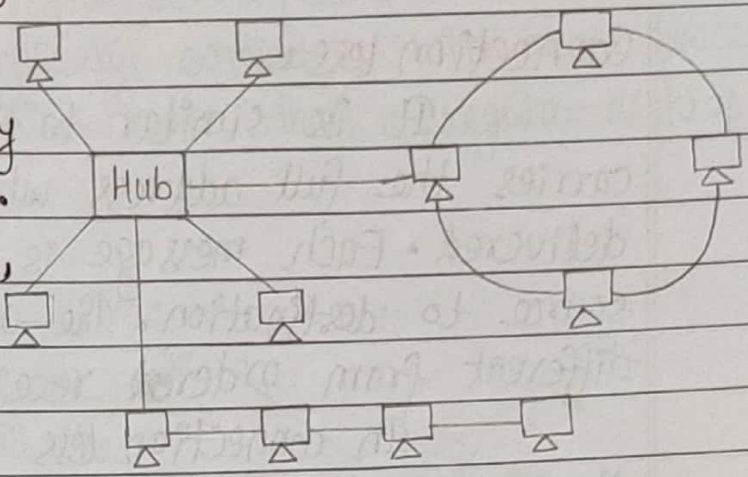


Fig: Hybrid Topology

Advantages: i) Inherits the advantages and disadvantages of topology included.
ii) Scalable as size can be increased easily.

Disadvantages: i) Complex in design.
ii) Costly.

Connection Oriented and Connection less Services

Connection Oriented:

There is a sequence of operation to be followed by the users of connection oriented service. These are:

i) Connection is established
ii) Information is sent
iii) Connection is released

In connection oriented service we have to establish a connection before starting the communication. When connection is established, we send the message or information

and then we release the connection. Connection Oriented service is more reliable than connection less service.
Example : TCP.

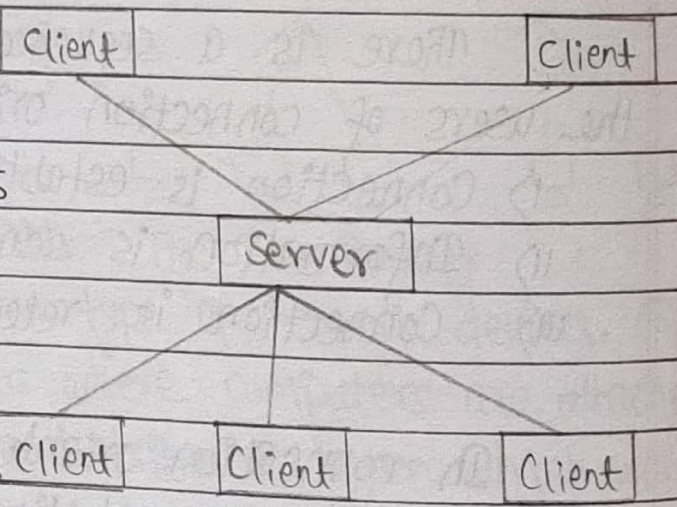
Connection less :

It is similar to the postal services as it carries the full address where the message is to be delivered. Each message is routed independently from source to destination. The order of message sent can be different from ordered received.

In connection less the data is transferred in one direction from source to destination without checking that destination is still there or not.
Example : UDP.

Network Architecture :

1. Client Server Architecture:

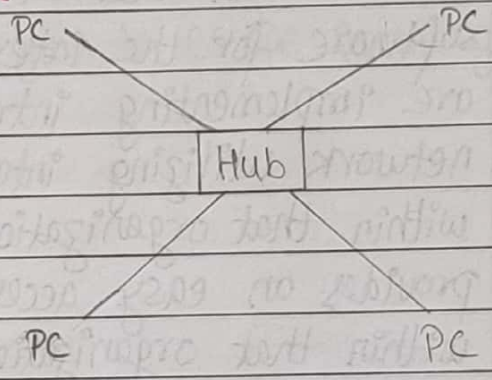


In a client server network, a number of network clients request resources or services from the network server. One or more network server manages and provide these resources or services. The client are computers that depend on the server

for data and software. Network server are also referred to as computer server or simply servers. Sometimes a server is described in terms of the specific service it provides, such as e-mail server, print server, file server, etc.

Servers are typically computers with more processing speed, memory and hard disk space than a regular desktop computer.

2. Peer-to-peer Architecture (P2P):



In P2P network, the task are allocated among all the members of the network. There is no real hierarchy among the computers and all of them are considered equal. This is also referred to as a distributed architecture or work group without hierarchy. A peer-to-peer network doesnot use a central computer server that control network activity.

Peer-to-peer is mostly used for file sharing and resource sharing.

Internet:-

It is a global system of interconnection of computers. It uses the standard internet protocol [TCP/IP. Every computer in internet is identified by an unique IP address. IP address is a unique set of number such as 110.132.032.111 which identifies a computer's location.

A special computer DNS (Domain Name Server) is used to provide a name to the IP address so that the user can locate a computer by a name. For example; a DNS server will resolve a name www.google.com to a particular IP address to uniquely identify the computer on which this website is hosted.

Intranet:-

With the advancement made in browser based software for the internet, many private organizations are implementing intranet. An intranet is a private network utilizing internet type tools but available only within that organization. For large organization an intranet provides an easy access mode to corporate informations within that organization.

- private network
- exist within the same company for branch locating
- has limited privilage.

Extranet:-

It can be defined as an extended intranet that links selected resource of a company within its customer and other business partners using the internet or private network to link the organization's intranet. It is a secure network that provides controlled access to areas of each others corporate intranet by remote authenticated parties. Example: ATM machine.

- semi-private network
- access is provided with limited privilege
- small internet form with authentication

VPN (Virtual Private Network):-

Basically, VPN is a private network that uses a public network (usually the internet) to connect remote users (nodes) together. Instead of using a dedicated real world connection, a VPN uses virtual connections routed through the internet from the company's private network to the remote site.

A VPN is typically a paid service that keeps your web browsing secure and private over public internet. VPN can also get pass for regional restrictions for video and music streaming websites and help you to escape from government restriction.

Advantages:

i) Improved security
ii) Encryption and decryption of data
iii) Hide IP address and geo-location.
iv) Reduce operational cost over traditional dedicated lines.

Protocol:-

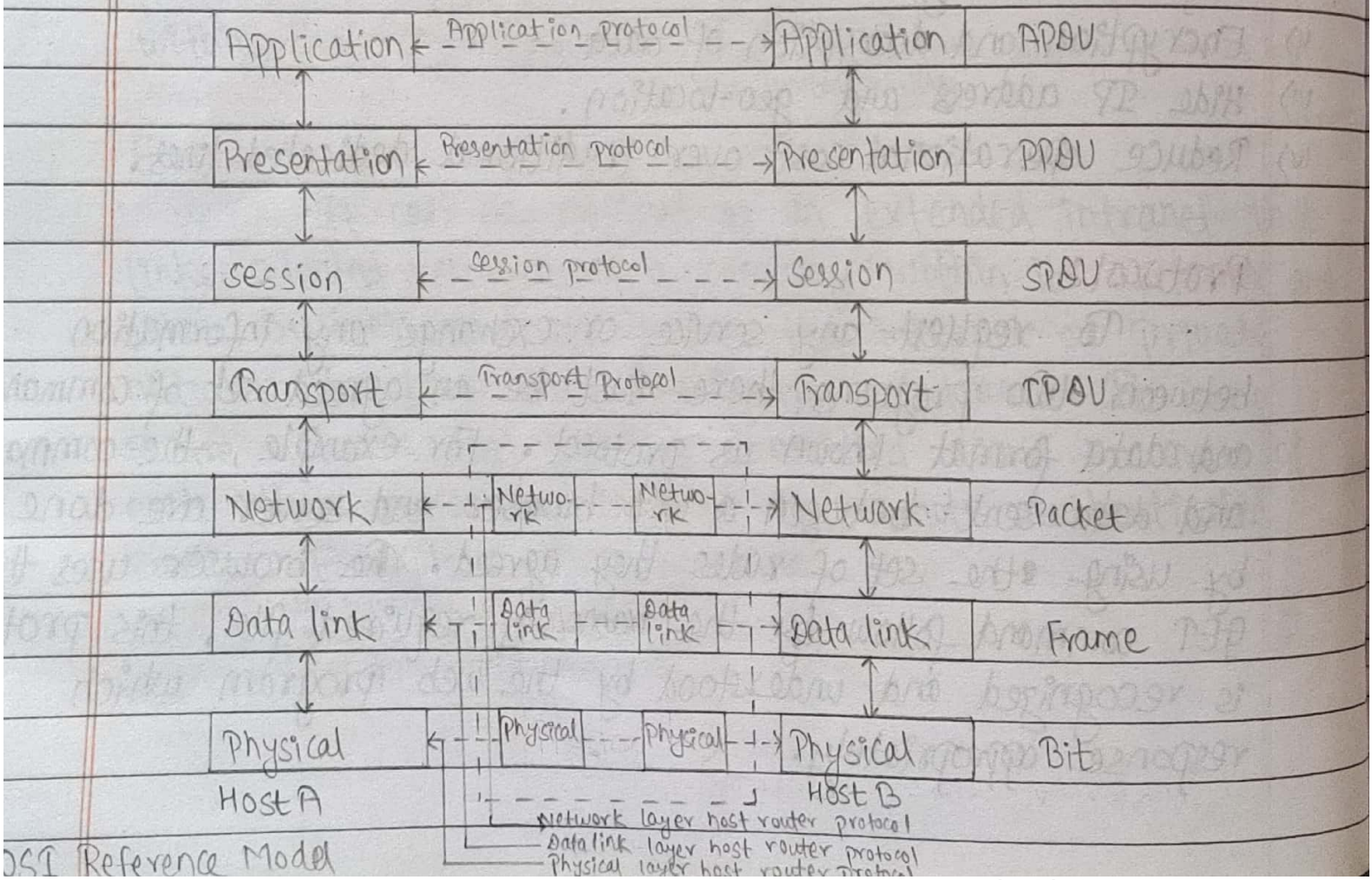
To request any service or exchange any information between two programs, there must be an agreed set of commands and data format known as protocol. For example, the commands and data sent between a web browser and server are done by using the set of rules they agreed. The browser uses the GET command follow by the name of required file, this protocol is recognized and understood by the web program which response appropriately.

Reference Model:

Reference model is a conceptual framework for understanding relationship between network parties. In reference model, there is a predefined structure for sharing information and resource over the network.

OSI Reference Model (Open System Interconnection):

This model is based on proposal developed by ISO (International Standard Organization) as a first step towards international standardization of the protocols used in the various layers. The model is called Open System Interconnection because it deals with connecting open systems i.e. system that are open for communication with other system.



OSI Reference Model

- bits are transmitted from source to destination (in form of electrical/optical/RF/microwave)
- Hub, repeaters, amplifiers (devices used in physical layer).
- Protocols are T_1, E_1, SOH/SONET, RS-232, etc.

1) Layer 1: Physical layer

It is the lowest layer of OSI model. Physical layer describes some type of cabling system as the transmission media. It also describes the network topology and how the transmission media is to be distributed. It activates, maintains and deactivates the physical connections.

The physical layer is concerned with transmitting raw bits over the communication channel i.e. with making sure that when one side sends one bit, it is received by the other side as one bit not as zero bit. Physical connection protocols decides how the initial connection is established, how it is turned down when both sides are finished.

11) Layer 2: Data link layer

Data link layer synchronizes the information which is to be transmitted over the physical layer. The main function of this layer is to make sure that data transfer is error free from one node to another over the physical layer. Transmitting and receiving data frames is managed by this layer. This layer sends and expects acknowledgement for frames received and sent respectively. Ascending of none acknowledgement received frames is also handled by this layer.

PDU - Protocol Data Unit

Encryption can be used to protect the message as it flows between each network node. Each node then decrypt the message received and re-encrypt it for transmission to the next node.

- Bits are assembled into frames and also encapsulates upper layer PDU into frames
- Hop to hop delivery of frame
- Error checking and recovery
- Physical addressing (MAC addressing)
- Protocols are PPP, frame relay, Ethernet, etc.
- device are switch, bridge, etc.

- Layer-3
- PDU are called packet
- End-to-end delivery of packets
- Logical addressing (IP addressing)
- Best path selection for delivery of packets from source to destination.
- devices :- router.
- protocols : IP, ICMP, IGMP, etc.

III) Layer 3 : Network layer

The network layer controls the operations of routing and decides by which node data should take. The network layer provides both connection oriented and connectless services. It divides the outgoing message into packets and assembles the incoming packets into messages for higher level.

All router in the network are operating at this level. If too many packets are present in the sub-net at the same time bottleneck will form. Network layer helps to control this congestion. An accounting function is build into the network layer to ensure that the number of bit send is equal to the number of bit received.

IV) Transport layer (layer 4) :-

This layer receives message from the session layer above it, convert the message into smaller units, passes it onto the network layer and ensure that the delivered data are the same as the data transmitted without modification, loss or duplication. If an error occurs during transmission, transport layer must correct it. There is a set of rules to follow the details, handling of the error, and how to correct it. The correction may means resending just the damaged data or restarting from the beginning. Transport layer decides that data transmission is either on parallel path or single path.

Transport layer breaks the message into small units so that they are handled more efficiently by the network layer.

- segmentation (PDU formed in Transport layer - segments) and reassembly.
- sequencing of segments.
- Port addressing
- Error checking and correction detection.
- Flow control | Congestion control.

v) Session layer (Layer 5):- - Initiates/ends session between services.

The session layer permits two parties to hold ongoing communication called a session across a network. The application on either end of the session can exchange data or send packet to another for as long as the session last. The session layer handles session setup, data or message exchanges and tear down when the session ends. It also monitors session identification so only designated parties can participate and security services to control access to session information.

The session has the option of proving one way or two way communication called control. Session can allow traffic to go in both direction at the same time or in only one direction at a time. Token management may be used to prevent both sides from attempting same operation at the same time. To manage these activities, session layer provides tokens that can be exchanged. Only the side holding the token is permitted to perform critical operation.

vi) Layer 6: Presentation layer

The presentation layer is responsible for the format of data transferred during network communication. This layer is concerned with syntax of information transferred. For outgoing messages, it converts data into a generic format for the transmission. For incoming messages, it converts data from the generic form to a format understandable to the receiving application. Different computers have different ~~course~~ codes for representing data. The presentation layer makes it possible for computers with different representation to communicate. - defines the way of presenting the data to the network.

- Data encryption/compression/encoding, etc.

- interface between human and network resource.
- Presents the application data to the end user.
- Protocols: HTTP, FTP, OIUS, etc.

vii) Layer 7: Application Layer

The application layer is the topmost layer of the OSI model. It provides a set of interfaces for applications to obtain access to network services as well as access to network services that supports application directly. This layer also provides application access security checking and information validation.

This is an end user interface that provides us a facility to enter commands that direct the applications to send files and receive files from remote host or to change, rename or delete files and directories. Eg: file zilla, github.

ISP (Internet Service Provider):-

An Internet Service Provider (ISP) is the industry term for the company that is able to provide you with access to the internet. If your hear someone talking about the internet and they mention their provider, they are usually talking about their ISP.

Your ISP makes the internet a possibility. In otherwords, you can have shiny computer with a built-in modem and could have a router for networking but without a subscription with an ISP, you won't have a connection to the internet. An ISP is your gateway to the internet and you will be able to send emails, go shopping, do research and many more. ISP is the link between your computer and all the other servers from the internet.

Internet backbone
Net Neutrality. } Assignment 1.

Internet backbone :-

An Internet backbone refers to one of the principal data routes between large, strategically interconnected networks and core routers on the Internet. An internet backbone is a very high-speed data transmission line that provides networking facilities to relatively small but high speed internet service providers all around the world.

Internet backbones are the largest data connections on the internet. They require high-speed bandwidth connections and high-performance servers/routers. Backbone networks are primarily owned by commercial, educational, government and military entities because they provide a consistent way for Internet service Providers (ISPs) to keep and maintain online information in a secure manner. Some of the largest companies running different parts of the Internet backbone include UUNET, AT&T, GTE Corp. and Sprint Nextel Corp. Their routers are connected with high-speed links and support different range options like T1, T3, OC1, OC3 and OC48.

A few key features of an Internet backbones include:

- ISPs are either connected directly to their contingency backbones or to some larger ISP that is connected to its backbone.
- The smaller networks are interlinked to support the multiversatile backup that is required to keep the Internet services intact in case of failure. This is done through transit agreements and peering processes.
- The transit agreement is a monetary contract between several larger and smaller ISPs. It is initiated to share traffic loads or to handle data traffic in case of a partial failure of some networks. In peering, several ISPs also share features and traffic burden.

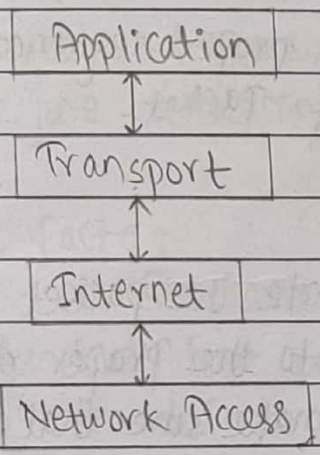
The first Internet backbone was named NSFNET. It was funded by the U.S government and introduced by the National Science Foundation (NSF) in 1987. It was a T1 line that consisted of approximately 170 smaller networks operated at 1.544 Mbps. The backbone was a combination of fiber-optic trunk lines, each of which had several fiber-optic cables wired together to increase capacity.

Net Neutrality:-

Net neutrality is the principle that governments should mandate Internet service Providers to treat all data on the Internet the same, and not discriminate or charge differently by user, content, website, platform, application, type of attached equipment, or method of communication. For instance, under these principles, internet service providers are unable to intentionally block, slow down or charge money for specific websites and online content. It is the principle that data packets on the Internet should be moved impartially, without regard to content, destination or source. The Net Neutrality principle holds that wired and wireless internet service is a utility like gas, water, electricity and landline phone service; it should be available to everyone and subject to government regulation. The term came from "Network Neutrality, Broadband Discrimination", a paper written by Columbia Law School Professor Tim Wu in 2003. According to him, the best way to explain network neutrality is that a public information network will end up being most useful if all content, websites and platforms (eg. mobile devices, video game consoles, etc.) are treated equally.

A more detailed proposed definition of technical and service network neutrality is the loyalty to the paradigm that operation of a service at a certain layer is not influenced by any data other than the data interpreted at that layer, and in accordance with the protocol specification for that layer.

TCP/IP Model:



TCP/IP Model is practical model and is used in internet. TCP/IP is acronym of Transmission control Protocol / Internet Protocol.

a) Application layer:

Application, Presentation and session layer of OSI model resides in this. Different type of applications handle different type of communication.

UDP : User Datagram Protocol

b) Transport layer:

The task of this layer is to establish the connection between the ~~peer~~ peer entities in the source and destination host. Two protocol resides in this layer; one is TCP which is reliable and the other one is UDP which is unreliable. TCP is also responsible for errorless transmission of data from source to destination. At the source, TCP divides the stream of bit it receives from upper layer and create packets and give it to the internet layer. At the destination, it assembles ~~to~~ the packets received in proper sequence even if the packet are received out of packet.

c) Internet layer:

The job of this layer is to create the packet which is known as datagram and ~~the~~ route it to the proper destination. It adds IP address to the packet to make sure that it reaches the correct destination. The protocol present in this layer is known as internet protocol. Different packets created in this layer may not follow the same path to reach the destination.

d) Network Access layer:

The job of this layer is to transmit the data given by upper layer from the host to the network to which the host is connected.

Standards:

Standards are essential in creating and maintaining an open and competitive market for equipment manufacturers and in guaranteeing national and international interoperability of data and telecommunication process. Standard provides guideline to manufacturers, vendors, government agencies and other service providers, to ensure the kind of interconnectivity necessary in today's market place and in international communications.

Data communication standards fall in two categories:

- De-facto (meaning by fact)
- De jure (meaning by law)

1) De facto:

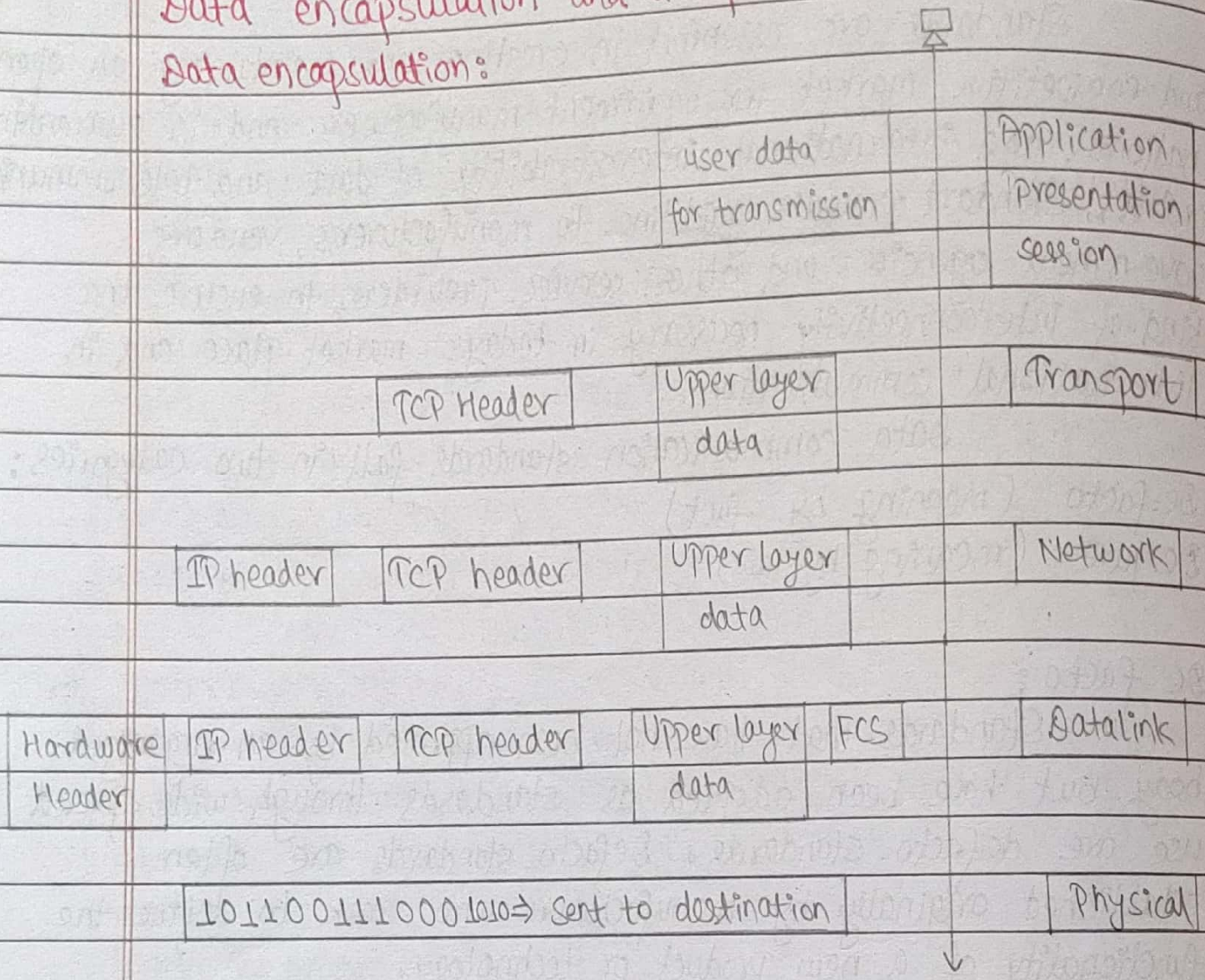
Standards that have not been approved by an organized body but have been adopted as standards through wide spread use are defacto standards. Defacto standards are often established originally by manufacturers who seek to define the functionality of a new product or technology.

11) Dejure:

Those standards that have been made by an officially recognized body are dejure standards.

Data encapsulation and decapsulation:

Data encapsulation:



The computer in the above figure needs to send some data to another computer. The application layer is where the user interface exists, here the user interact with the application he/she is using, then this data is passed to the presentation layer and session layer. These three layers adds some extra information to the original data that came from the user and passes it to the transport layer. Here, the data is broken into smaller pieces (one piece at a time is transmitted) and the TCP header is added. At this point, the data at the transport layer is called

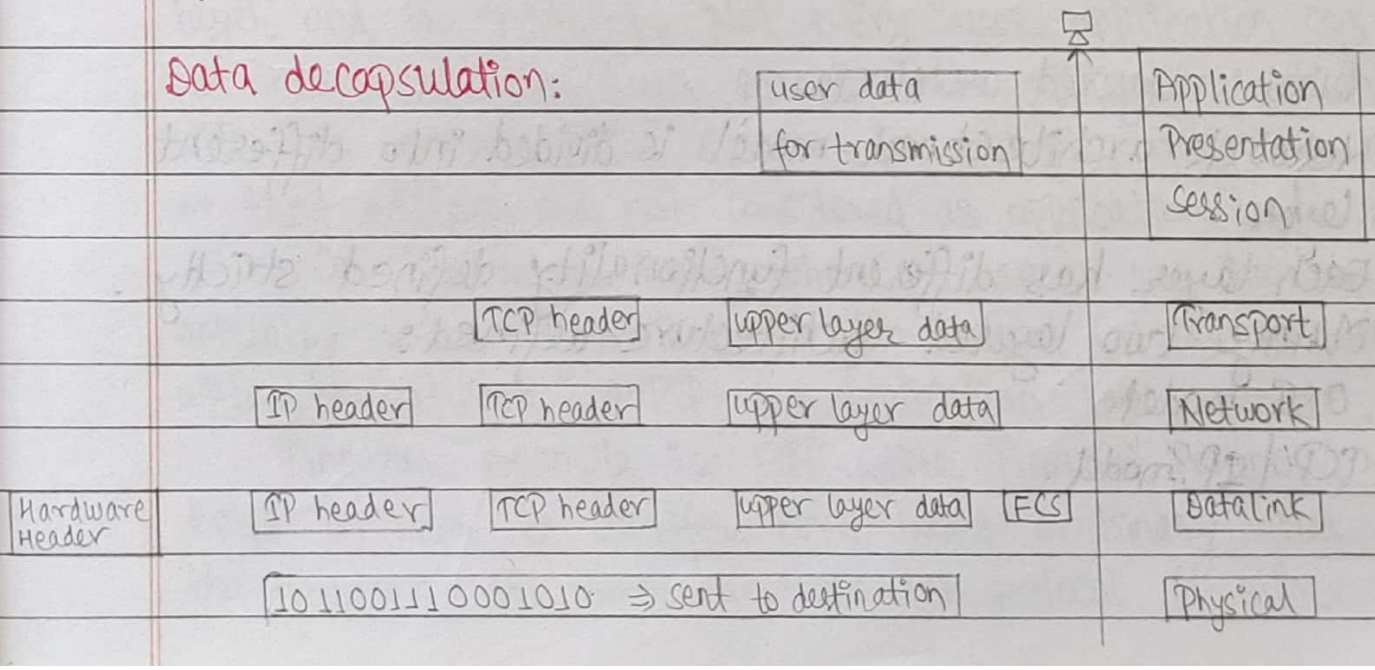
a segment.

Each segment is sequenced so the data stream can be put back together on the receiving side exactly as transmitted. Each segment is then handled to the network layer for network addressing and routing. At the network layer, we call the data a packet.

The network layer add its IP header and then sends it to the datalink layer. Here we call the data a frame. The data link layer is responsible for taking packets from the network layer and placing them on the network medium (cable). The datalink layer encapsulate each packet in a frame which contains the hardware address of source and destination which identifies to which protocol in the previous layer (network layer) the packet should be passed when it arrives to its destination. Also at the end, you will notice the FCS (Frame check sequence). This is used for error checking and is also added at the end by datalink layer.

Frame is a logical group of ones and zero's, the physical layer is responsible for encapsulating these digits into a digital signal which is read by devices on the same local network.

Data decapsulation:



The receiving computer will firstly synchronize the given bits. Once the synchronization is complete and it receives the whole frame and passes it to the data link layer. The datalink layer will do a cyclic redundancy check on the frame. This is a computation which occurs in network to match the value i.e. the frame has been received without any errors. Now, we are moving from the datalink layer to the network layer. At the network layer, the IP address is checked and if it matches the IP header then the IP header is released from the packet and rest is passed to the above layer which is transport layer. Here, the rest of the data is now called a segment.

The segment is processed at the transport layer, which re-builds the data stream (at this level on the senders computer it was actually split into pieces so they can be transferred) and acknowledges to the sender from this layer that we are using TCP not UDP. After all that, it then hands the data stream to the upper layer application.

Q. What is layered architecture?

⇒ Network architectural model is divided into different layer.

- Each layer has different functionality defined strictly.
- Mainly two layered architecture defined:

i) OSI model
ii) TCP / IP model.

1.3

Application layer:-

Application layer is the top most layer of OSI and TCP/IP layered model. This layer exist in both layered models because of its significance of interacting with user and user application. This layer is for applications which are involved in communication system.

Application layer is where the actual communication is initiated and reflects. Because this layer is on the top of the layer stack, it doesnot serve any other layers. Application layer takes the help of transport and all layers below it, to communicate or transfer its data to the remote host. When an application layer protocol wants to communicate with its peer application layer protocol on the remote host, it hands over the data to transport layer.

There is an ambiguity in understanding application layer and its protocol. Not every user application can be put into application layer except those applications which interact with the communication system. For example; designing softwares or text editors are not considered as application layer programs.

On the other hand, when we use a web browser which is actually using Hyper Text Transfer Protocol (HTTP) to interact with the network, HTTP is an application layer protocol.

Another example is FTP (File Transfer Protocol) which helps an user to transfer text based or binary files across the network. The user can use this protocol in either GUI

(Graphical User Interface) based software like filezilla and same user can also use command line mode.

Hence, irrespective of which software you use, it is the protocol which is considered at application layer used by that software. DNS (Domain Name System) is a protocol which helps user application protocols such as HTTP to accomplish its work.

DNS (Domain Name System):

The Domain Name System (DNS) works on client/server model. The DNS server is configured with fully qualified domain name (FQDN) mapped with their respective internet protocol (IP) addresses, DNS helps to resolve the host name to an address. It uses a hierarchical naming scheme and distributed database of IP addresses and associated names.

DNS Architecture:

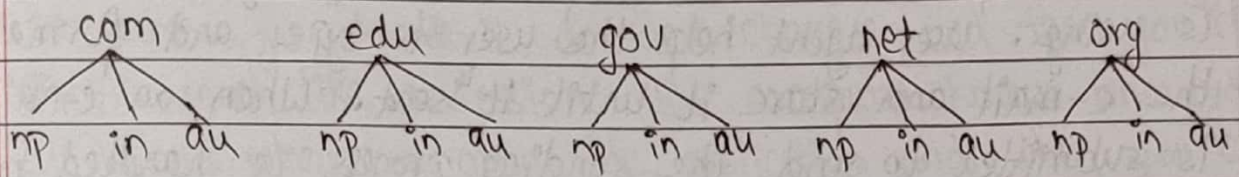
The domain name system comprises of domain names, ~~name servers~~ domain name space, name server.

Domain Name:

Domain Name is a symbolic stream associated with an IP address. There are several domain names available, some of them are generic such as com, edu, gov, etc while some country level domain name such as np, au, in, etc.

Domain Name Space:

The Domain Name Space refers a hierarchy in the internet naming structure.



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.

HTTP :-

The Hypertext Transfer Protocol (HTTP) is the foundation of world wide web (WWW). Hypertext is well organized documentation system which uses hyperlinks to link the pages in the text document. HTTP works on client-server model. When a user wants to access any HTTP page on the internet, the client machine at user end initiates a TCP connection to server on port 80. When a server accept the client request, the client is authorized to access webpages.

To access the webpages a client normally uses web browser who are responsible for initiating, maintaining and closing TCP connections. HTTP is a stateless protocol that means server does not maintain information about earlier request.

Client (Program matching data mail server ma data storage

SMTP (Simple Mail Transfer Protocol) :-

The Simple Mail Transfer Protocol is used to transfer electronic mail from one user to another. This task is done by means of e-mail client software (user agent) the user is using. User agent helps the user to type and format the e-mail and store it until it is sent. When an e-mail is submitted to send, the sending process is handled by user agent which is normally comes in-build.

SMTP is limited in its ability to queue message at the receiving end, it is usually used with one of two other protocols POP (Post Office Protocol) or IMAP (Internet Messaging Access Protocol), that let the user save messages in the server mail box and download them periodically from the server. In other words, user typically uses a program that uses SMTP for sending e-mail and either POP or IMAP for receiving e-mail.

File Transfer Protocol (FTP):-

The file transfer protocol (FTP) is most widely used protocol for file transfer over the network. FTP uses TCP/IP for communication and it works on port 21. FTP works on client-server model where a client request file from server and server sends requested resource back to the client.

The client request the server for a file. When a server receives a request, it opens a TCP connection for the client and transfer the file. After the transfer is complete, the server closes the connection. For a second file, client request again and

server re-opens a TCP connection.

Session :-

When you are working with an application on your computer, you open it, do some changes and then you close it. This is much like a session. The computer knows who you are. It knows when you open the application and when you close it. However, on the internet there is one problem : the web server does not know who you are and what you do because the HTTP address doesnot maintain state.

Programming languages solves this problem by creating a unique cookie for each other. The cookie is sent to the users computer and it contains information that identifies the user.

Variables stored in a session object hold information about one single user, and are available to all pages in that application. Common information stored in session variable are name, id, email, phone, etc.

When user starts an application, the session will start and user will see the output according to that session object. If a user has not requested or refreshed a page in the application for specified period by default session will destroy itself.

Cookie :-

Cookies are small files that are saved to your browser when visiting a website. They can store previous activity on that site so that this information can be retrieved the next time you visit the same site. It is recommended that you clear your browsers cookie every few weeks to keep it running efficiently. You may want to configure your browser setting for not to accept cookies or remove cookies upon closing or exiting the browser window.

Eg:

```
color = "red" expires = "10 March 2018 00:00:00 UTC";
```

In the above example, cookie has named value pairs. The expire attribute specifies when the cookie is going to be expired.

fast execution

Cache :-

Browser cache a temporary internet files are a way that browsers download websites, image, data, document for faster viewing in the future. By keeping a local copy of some website information, your browser will be able to load at least some information from each page you have visited without downloading that information again from the server. This can decrease the time it takes to load a webpage. The downside is that the information on a website may have changed while your browser loads an older version. It is recommended that you clear your browsers cache

every few weeks to keep it running efficiently.

Reliable Data Transfer:-

The network layer for a protocol stack is responsible for getting a message from the source machine to the destination machine. However there are often several programs running on the source machine and several programs running on the destination machine. The transport layer for a protocol stack is responsible for getting the message to the right program on the destination machine. On the internet, there is one main protocol for the network layer called IP (Internet Protocol). However on the internet there are two alternative protocols for the transport layer called TCP and UDP. TCP is used by many of the applications because it guarantees reliable delivery.

Protocols on Reliable Data Transfer:

single data at a time transfer garxa.

1) Reliable Data Transfer Protocol : Stop & Wait

These protocols re-transmit a data packet if acknowledgement indicates that the data packet may not have been successfully transmitted during the previous attempt.

When sender sends one data packet and at the other end receiver receives that data packet, the receiver checks to see if the data packet has been corrupted. If the data packet has not been corrupted then the receiver sends a positive acknowledgement packet back to the sender. When the sender receives an acknowledgement, the sender

can then send the next data packet.

What happens in the stop and wait protocol if something goes wrong? One case is when the sender's packet is lost or corrupted. In this case, the sender has to recognize that the data packet needs to be retransmitted. Notice that the receiver will not send an acknowledgement if the data packet has been lost or corrupted. Consequently, the sender can use a time-out period. The time-out period starts when the data packet is sent. If the sender does not receive an acknowledgement packet by when the time-out period expires and retransmits the data packets. The receiver will then receive a second copy of data packet and discard one of them and retransmit the acknowledgement packet.

multiple frame lai sangai pathauxa.

II) Reliable Data Transfer Protocol : Pipelined (Selective Repeat)

In a pipelined reliable data transfer protocol, the sender can start sending a second data packet before the sender receives the acknowledgement for the first data packet. Thus if the sender needs to send several data packets, then the time until the last of the packet is shorter with a pipelined protocol. Thus, a pipelined protocol can have better performance than the stop and wait protocol. The sender can keep on sending packets even if the acknowledgement for the earlier packets have not yet returned. Thus it takes less time to send the sequence of packets.

Errors can occur when a pipelined protocol is used, just as they can occur in stop and wait protocol. The

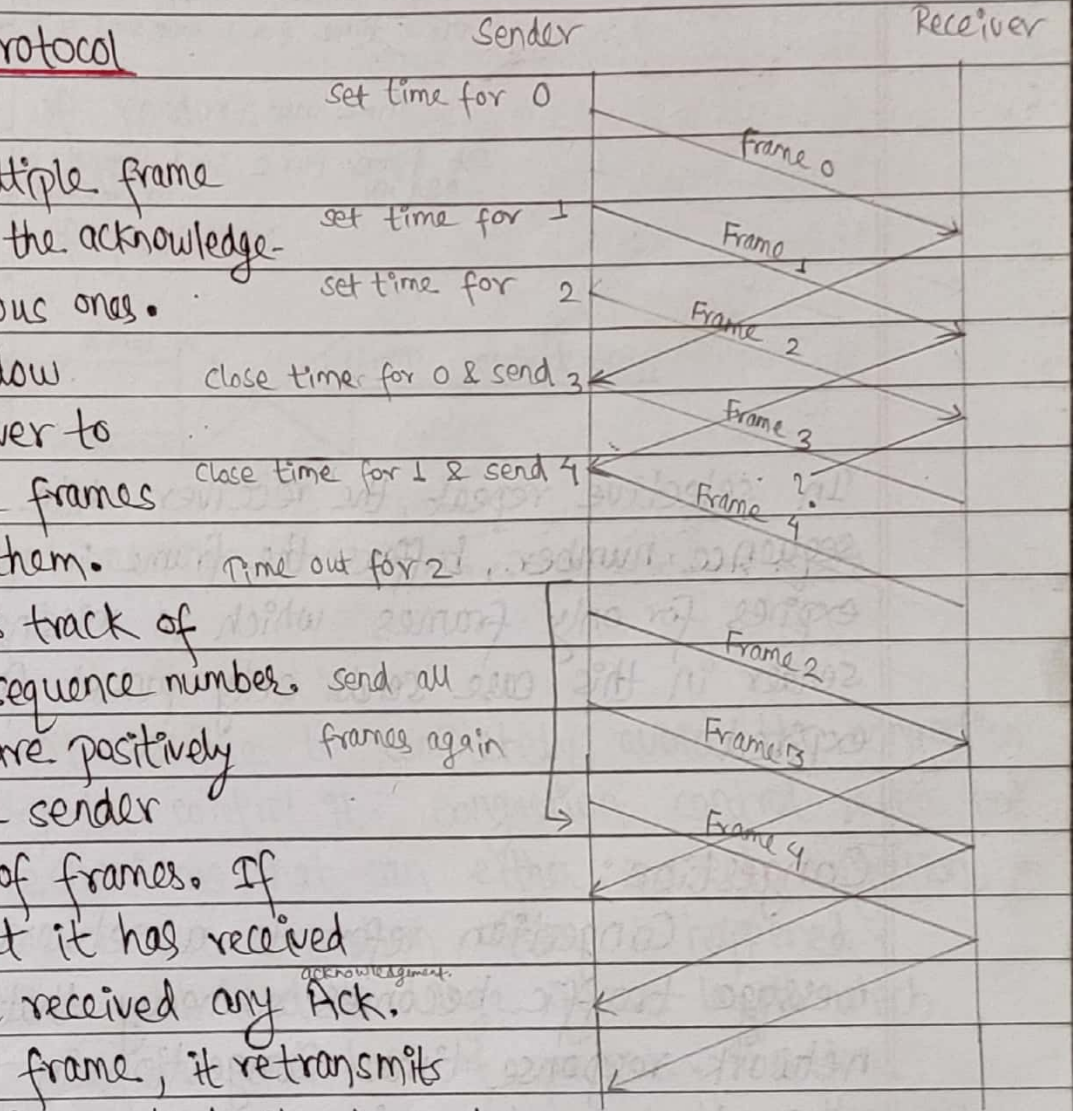
same two cases exist.

a) A lost or corrupted data packet
b) lost or corrupted acknowledgment signal.

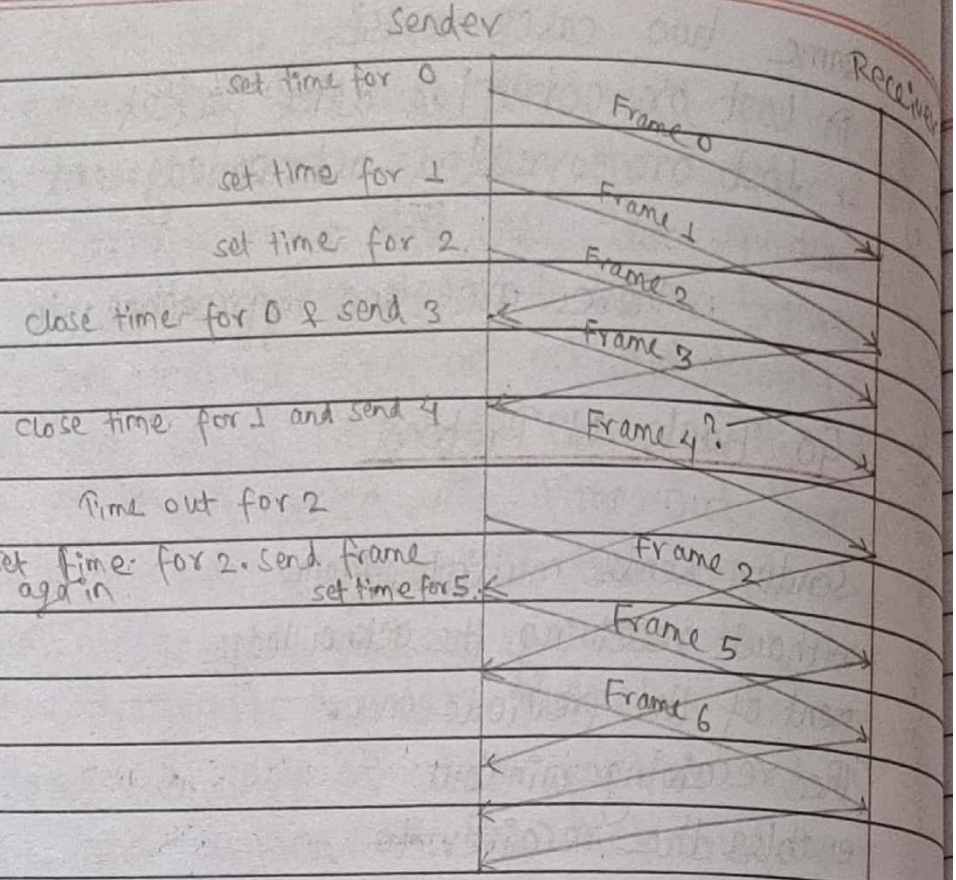
There are two approaches to solve these problems:

Go Back N Protocol

Sender sends multiple frame 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 frames sequence number. If all frames are positively acknowledge, the sender send next set of frames. If sender finds that it has received Nack or has not received any Ack. for a particular frame, it retransmits all the frame after which it does not receive any positive acknowledgement.



Selective Repeat



In selective repeat, the receiver while keeping track of sequence number, buffers the frame in memory and time-out expires for only frames which is missing or damaged. The sender in this case sends only packet for which time.out was expired

Congestion:

Congestion refers to a network state in which the message traffic becomes so heavy that it slows down network response time. Congestion in a network may occur when the number of packets sent to the network is greater than the number of packets a network can handle.

Causes of Congestion:

1. Data from multiple input lines at the same time:

   If data arrives from multiple input lines at the same time and all need the same output line, then the input traffic rate exceeds the capacity of the output lines and as a result a queue gets build up.

2. Slow performance of router:
3. Router buffer limitation
4. Slow performance of processor

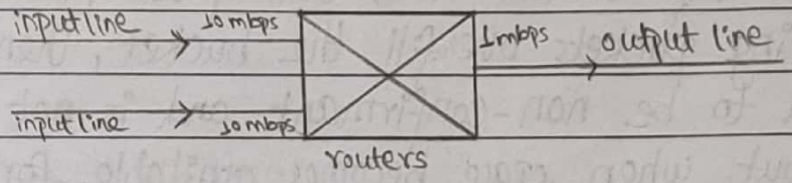


Fig: Congestion

Congestion control & its need:

It is not possible to completely avoid the congestion but it is necessary to control it. Congestion control refers to techniques and mechanisms that can either prevent congestion, before it happens or remove congestion after it happened.

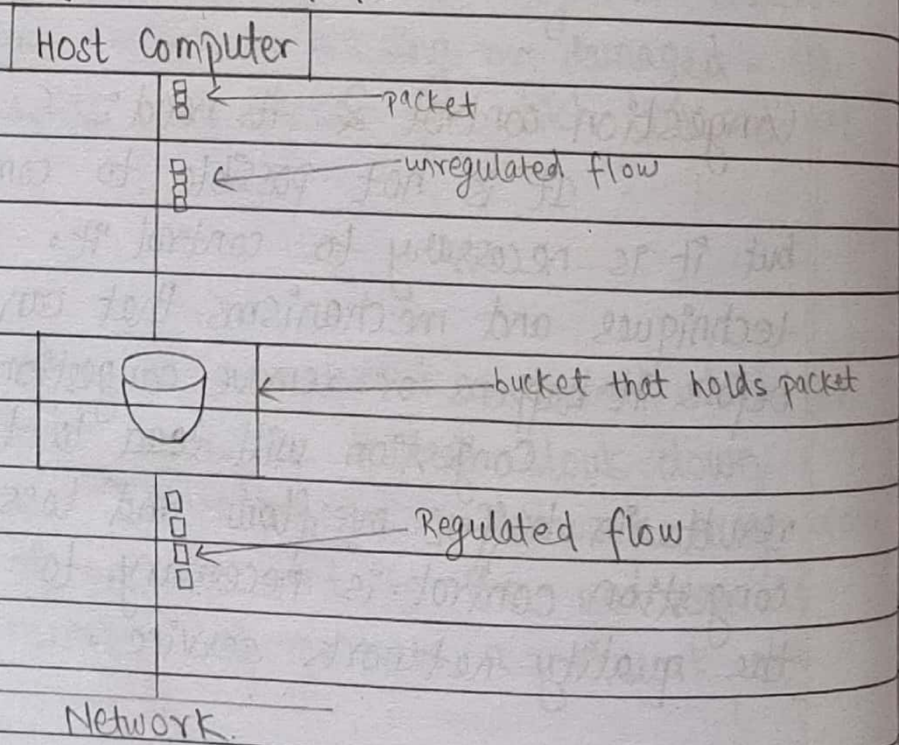
Congestion will lead to large queue length which results in buffer overflow and loss of packets. Therefore, congestion control is necessary to ensure that the user gets the quality network service.

Congestion Control Algorithms:

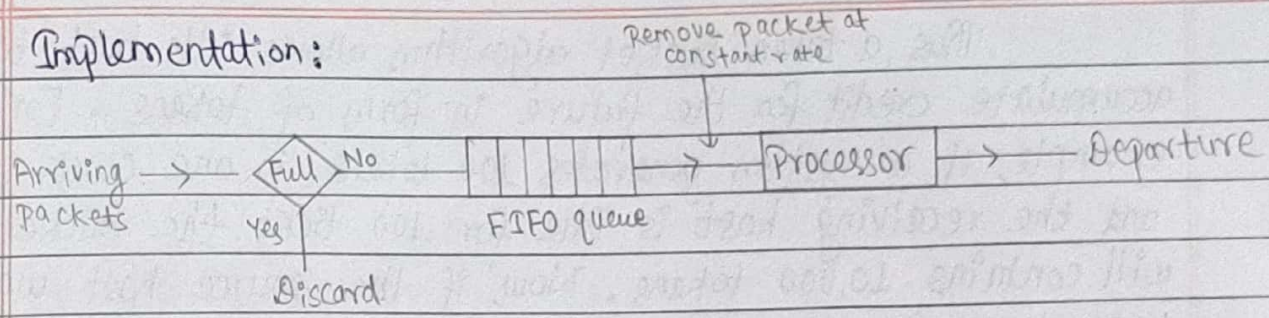
1. Leaky bucket algorithm:

A leaky bucket algorithm is a traffic shaping mechanism that shapes burst traffic into fixed rate traffic by averaging the data rate. The working mechanism of the algorithm is exactly similar to a leaky bucket and hence the named. Conceptually each network interface contain a leaky bucket which is a finite queue that outputs a finite rate.

When the bucket runs out of data, the leakage stops. If incoming packets overfill the bucket, then the packets considered to be non-confirmant and is not added to the bucket but when space becomes available for confirming packets, they are added to the bucket.



Implementation:

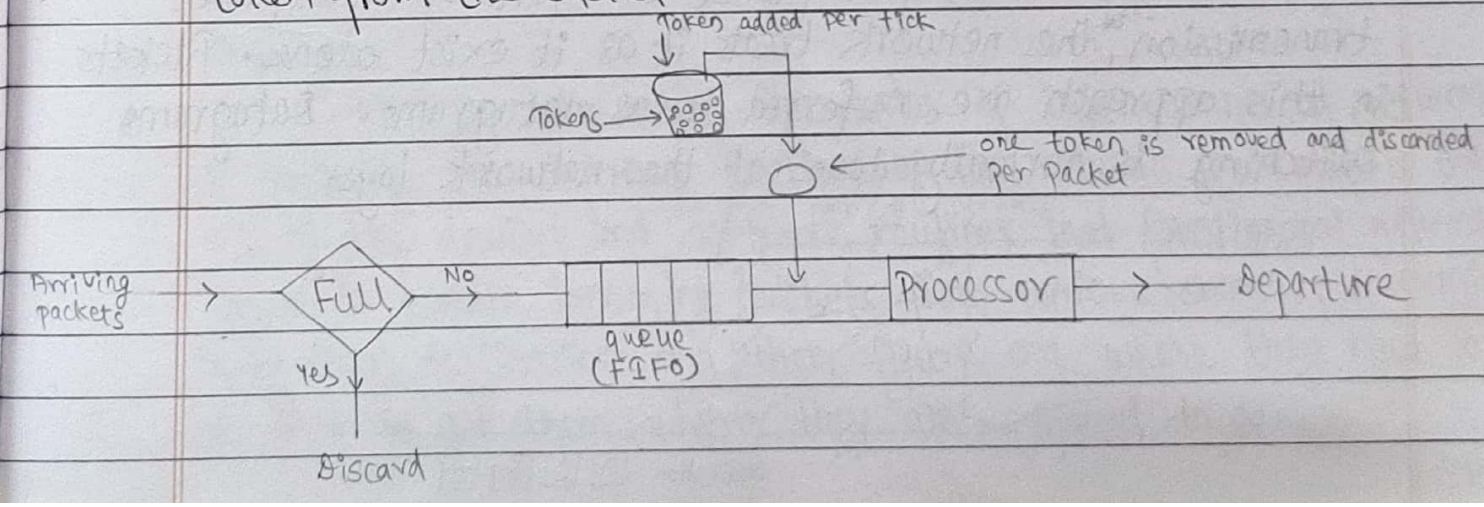


Implementation of the algorithm is easy and consists of a finite queue. Whatever a packet arrives, if there is a space in the queue it is added to the queue and if there is no space the packet is discarded.

2. Token Bucket Algorithm:

To overcome the limitation of leaky bucket algorithm, a token bucket algorithm is introduced which is a modification of leaky bucket algorithm in which bucket contains token.

In this algorithm, tokens are generated at every clock tick and added to the bucket in the constant rate. For a packet to be transmitted system must capture and destroy one token from the bucket.



Thus, a token bucket algorithm allows idle host to accumulate credit for the future in form of tokens. For example; if a system generates 100 tokens in one clock tick and the receiving host is idle for 100 ticks, the bucket will contains 10,000 tokens. Now, if the source host wants to send the bursty data, it can consume all 10,000 tokens at once for sending 10,000 packets.

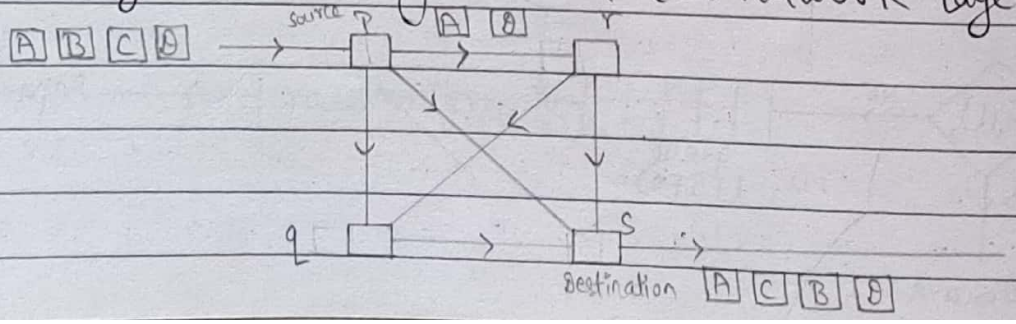
Implementation of Token Bucket Algorithm:

i) A token bucket algorithm can be easily implemented with a counter.
ii) The token is initialized to 0.
iii) Each time a token is added and the counter increments by 1 and each time when a unit of data is dispatched, the counter is decremented by 1.
iv) If the counter contains 0, the host cannot send any data.

network ma
every packet independently treat hunxa, afno path aafai determine garxa,

Datagram Network:

In a datagram network, each packet is treated independently. Even if a packet is a part of multipacket transmission, the network treats it as if it exist alone. Packets in this approach are referred to as datagrams. Datagrams switching is normally done at the network layer



Network Layer

Third layer of OSI model is a network layer. Network layer manages host and network addressing, managing sub networks and inter-networking.

Network layer takes the responsibility for routing packets from source to destination within or outside the sub-net.

Network layer functions:

1) **Logical addressing:**

On the internet, the internet protocol IP is the network layer protocol and every networking devices is assigned with an IP address. Note that, addressing is done at the data link layer as well but those address refers to local physical address.

2) **Routing:**

Moving data across the series of inter-connected networks is probably the defining function of the network layer. It is the job of the devices and software routines that function at network layer to handle incoming packets from various sources, determine their final destination and then figure out where they need to be sent to get them where they are supposed to go.

iii) Fragmentation and reassembly:

The network layer must send messages down to the datalink layer for transmission. Some datalink layer technologies have limits on the length of any message that can be sent. If the packet that the network layer wants to send is too large, the network layer must split the packet, send each piece to the datalink layer and then have pieces re-assembled once they arrive at the network layer on the destination.

iv) Error handling and diagnostic:

Special protocols are used at the network layer to allow devices that are logically connected, or that are trying to route traffic, to exchange information about the status of the host on the network

sender bata receiverma data pathauda kun path use garne

Packet Switching:-

Packet switching is a digital networking communication method that group all transmitted data into suitable sized blocks called packet, which are transmitted via a medium that may be shared by multiple simultaneous communication sessions. Packet switching increases network efficiency. Packet switching may be classified into connectionless packet switching also known as datagram switching and connection oriented packet switching also known as virtual circuit switching.

In datagram switching, each packet includes complete addressing information. Each packet are labelled with

a destination address, source address and are routed individually. It may also be labelled with a sequence number of the packet. This prevents the need for a dedicated path to help the packet find its way to its destination, but means that much more information is needed in the packet header which is therefore occupy larger memory buffer.

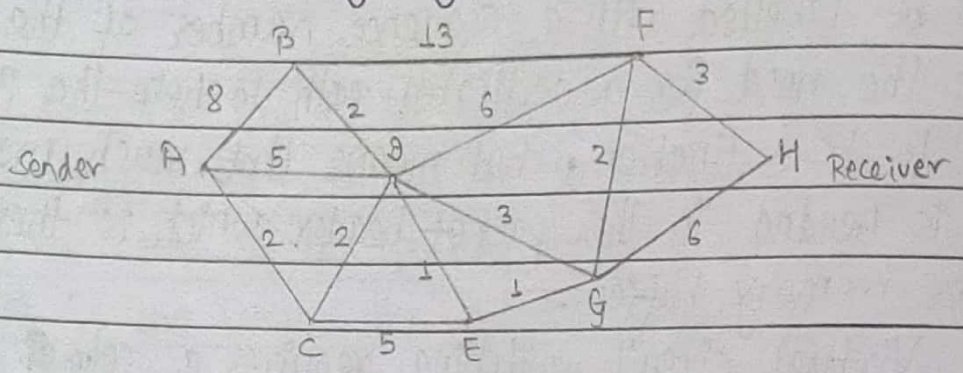
Virtual circuit switching requires a setup phase in each involved node before any packet is transmitted to establish the parameters of communication. The packet include a connection identifier and are negotiated between end points so that they are delivered in order with error checking. Address information is only transferred to each node during the connection setup phase. Routing a packet requires the node to look up the connection ID in a table. The packet header can be small as it only needs to contain source address, destination address and path to follow.

jaba data le source bata destination ma jada dherai path vetaucha, taba kun path jane vanne kura routing principle le determine garxa.

Routing Principle:

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. There are different types of routing algorithm.

1) Link State Routing Algorithm: (Dijkstra's Algorithm)



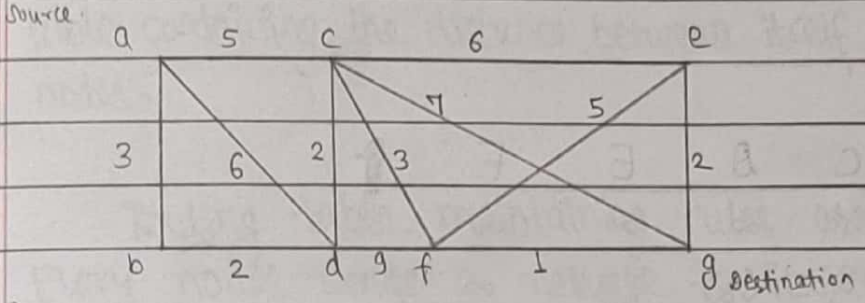
	A	B	C	D	E	F	G	H
A	0_A	8_A	2_A	5_A	∞	∞	∞	∞
C		8_A	2_A	4_C	7_C	∞	∞	∞
D		6_D		4_C	5_D	10_D	7_D	∞
E		6_D			5_D	10_D	6_E	∞
B		6_D				10_D	6_E	∞
G						8_G	6_E	12_G
F						8_G		11_F
H								11_F ← final destination.

Shortest path for above network is A-C-D-E-G-F-H.

Link State Routing is a complex routing technique in which each router shares information with other routers about the reachability of other networks and the metric (unit/cost) to reach the other networks in order to determine the best path. The metric is based on number of hops, link speeds, traffic congestion and other factors. A hop is the trip that a packet takes from one router to another as it traverses a network on the way to its destination.

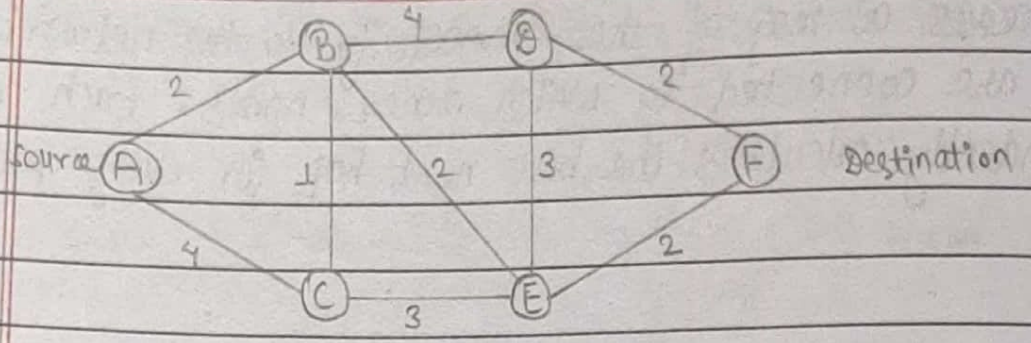
In link state routing, every router on the

network receives a map of the connectivity to the network showing which nodes are connected to which other nodes. Each router then independently calculates the best next hop for every possible destination.



	a	b	c	d	e	f	g
a	[0a]	3a	5a	6a	∞	∞	∞
b		[3a]	5a	5b	∞	∞	∞
c			[5a]	5b	11c	8c	12c
d				[5b]	11c	8c	12c
f					11c	[8c]	9c
g							[9f] ← final destination

Shortest path for above network is a - c - f - g.



Sol:

	A	B	C	D	E	F
A	$\boxed{0_A}$	2_A	4_A	∞	∞	∞
B		$\boxed{2_A}$	3_B	6_B	4_B	∞
C			$\boxed{3_B}$	6_B	4_B	∞
E				6_B	$\boxed{4_B}$	6_E
D				$\boxed{6_B}$		6_E
F						$\boxed{6_E}$ ← final destination

2) Distance Vector Routing Algorithm:

A router transmits its distance vector to each of its neighbours in a routing packet.

Each router receives and saves the most recently received distance vector from each of its neighbour. A router recalculates its distance vector when:

- It receives a distance vector from a neighbour containing different information than before.
- It discovers that a link to a neighbour has gone down using trigger update.

Distance vector Routing Algorithm:

- By periodic update

Note: Bellmans Protocol :-

Each router maintains a distance vector table containing the distance between itself and all possible destination nodes.

Routing table maintaining rules are:

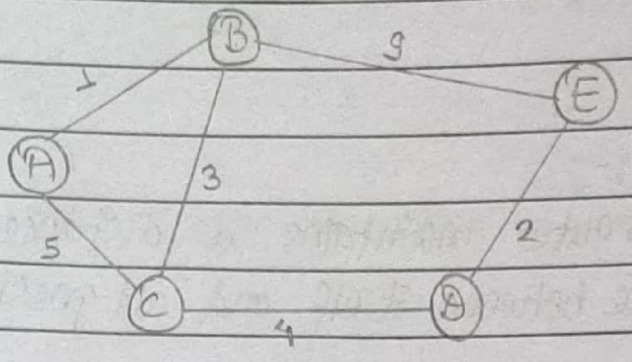
i) Every nodes sends a message to its directly connected neighbour containing its personal list of distance.

ii) If any of the receipient of the information from node x, find that node x is advertising a path shorter than the one they currently know about, they update their list to give the new path length and note that they should send packets for that destination through node x.

iii) After every node has exchanged a few updates with its directly connected neighbours, all nodes will know the least cost path to all the other nodes.

iv) In addition to updating their list of distances when they receive updates, the nodes need to keep track of which node told them about the path that they used to calculate the cost, so that they can create their forwarding tables.

Hop - intermediate node | direct node
multi-node



Reference, Node C

Destination	Cost	Hop
A	5	A
B	3	B
D	4	D

Reference from A

To	
A	0
B	1
C	5

Calculation with Reference of A

Dest	Cost	Hop
A	5	A
B	3	B
D	4	D

Reference from B

To	
A	1
B	0
C	3
E	9

Calc with

Reference of B

Destination	Cost	Hop
A	4	B
B	3	B
D	4	D
E	12	B

Reference from D

To	
C	4
D	0
E	2

Destination	cost	Hop
A	4	B
B	3	B
D	4	[illegible]
E	6	[illegible]

3) Hierarchical Routing:

As networks grow in size, the router's routing table grows proportionally. Not only the router's memory consumed by ever increasing tables, also more CPU time is needed to scan them and more bandwidth is needed to send status report about them. The network may grow to the point where it is no longer feasible for every router to have an entry for every other router.

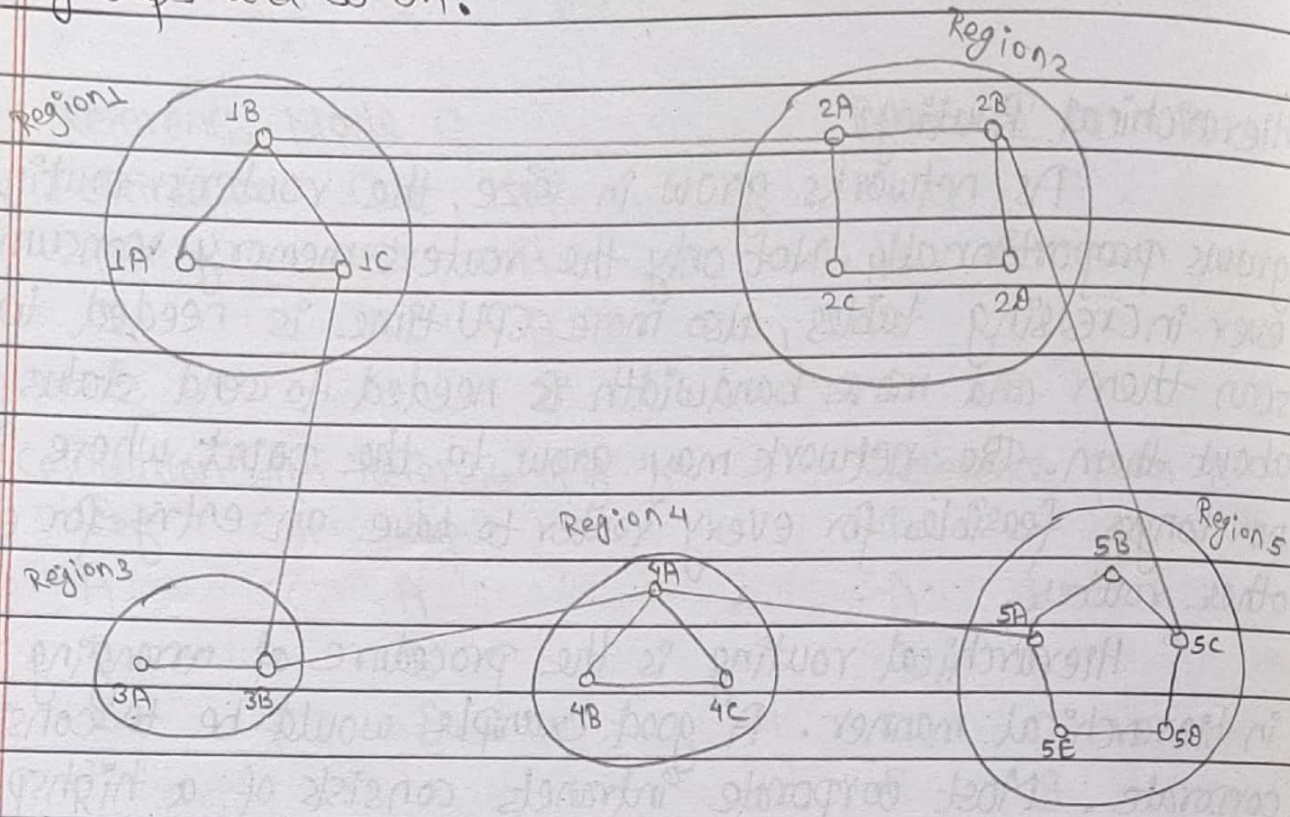
Hierarchical routing is the procedure of arranging routers in hierarchical manner. A good example would be to consider a corporate. Most corporate intranets consists of a highspeed backbone network. Connected to this backbone are routers which are in turn connected to a particular work groups. These work groups occupy a unique network. The reason that is ~~the~~ a good arrangement is because even though there might be dozens of different work groups, the span (maximum hop count to get from source host to destination host) is two.

Working principle:

In a network, the router are divided into regions. Each router knows all the details about how to route packets

to destination within its region but knows nothing about the internal structure of other regions.

For huge network, a 2-level hierarchy may be insufficient; it may be necessary to group the regions into clusters, the clusters into zones, the zones into groups and so on.



Destination	Line	Hops
1A	-	-
1B	1B	1
1C	1C	1
2	1B	2
3	1C	2
4	1C	3
5	1C	4

Internet Protocol (IP) :-

The Internet Protocol (IP) is the method by which data is sent from one computer to another on the network. Each computer (known as host) on the internet has at least one IP address that uniquely identifies it from all other computers on the internet.

The message sent by sender is divided into a number of packets, each packet can, if necessary be sent by different route across the internet. Packets can arrive in a different order than the order they were sent in. The internet protocol just delivers them to a destination.

IP is a connection less protocol which means that there is no continuing connection between the end points that are communicating. Each packet that travels through the internet is treated as an independent unit of data without any relation to any other unit of data.

The most widely used version of IP today is Internet Protocol version 4 (IPV4). However, IP version 6 (IPV6) is also beginning to be supported. IPV6 provides for much longer addresses and therefore for the possibility of many more internet users. IPV6 includes the capabilities of IPV4 and any server that can support IPV6 packets can also support IPV4 packets.

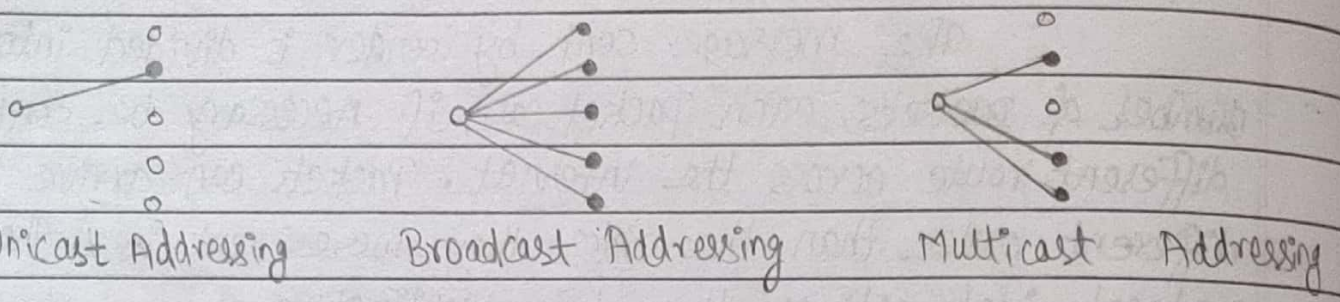
IPV4 :-

IPV4 provides a mechanism to uniquely identify host by an IP addressing scheme. IP uses best effort delivery i.e. it does not guarantee that packets would be delivered to the

destined host, but it will do its best to reach the destination. IPV4 uses 32-bit logical addresses.

IPV4 Addressing (IP section):-

IP supports the following services



Unicast Addressing Broadcast Addressing Multicast Addressing

1) Unicast Addressing:-

Unicast is the term used to describe communication where a piece of information is sent from one point to another point. In this case, there is just one sender and one receiver.

Unicast transmission in which a packet is sent from a single source to a specified destination, is still the pre-dominant form of transmission within the internet.
Example: HTTP, FTP, SMTP, etc.

1) Broadcast Addressing:-

Broadcast is the term used to describe communication where a piece of information is sent from one point to all other points. In this case, there is just one sender but the information is sent to all connected receivers.
Example: UDP.

iii) Multicast Addressing :-

Multicast is the term used to describe communication where a piece of information is sent from one point to a set of selected other points. In this case, the information is distributed to a set of receiver

Example : TCP.

multiple signal lai euta; signal ma transmit garne

Multiplexing & Demultiplexing :-

Multiplexing is the set of techniques that allows the simultaneous transmission of multiple signals across a single data link. Whenever the transmission capacity of a medium linking two devices is greater than the transmission needs of the devices, the link can be shared in order to maximize the utilization of the link, such as one cable can carry a hundreds channels of TV.

Demultiplexing is a set of techniques that separates single multiplexed signal through the communication link to individual signals.

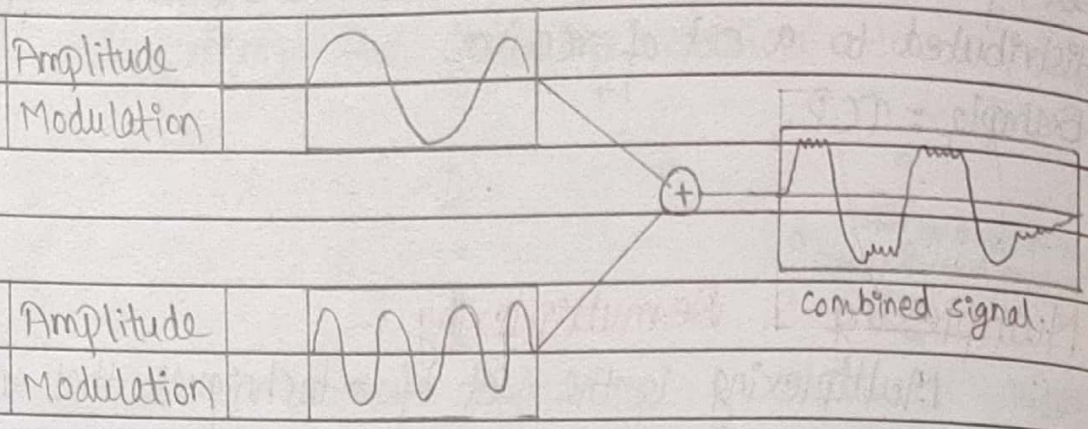
Types of Multiplexing:

1) Frequency Division Multiplexing (FDM)
2) Time Division Multiplexing (TDM).

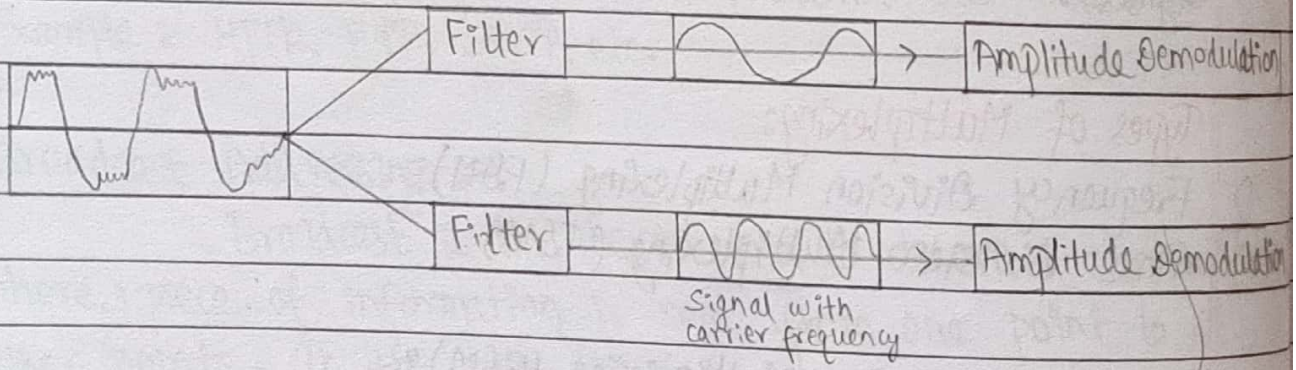
1) Frequency Division Multiplexing (FDM) :-

In FDM, signals generated by each sending devices modulate different carrier frequencies. These modulated signals are then combined into a single composite signal that can be transported

by the link. The carrier frequencies have to be different enough to accomodate the modulation and demodulation signal.



In demultiplexing process, we use filters to decompose the multiplexed signal into its constituent component signals. Then each signal is passed to an amplitude demodulation process to separate the carrier signal from the message signal. Then the message signal is sent to the waiting receiver.



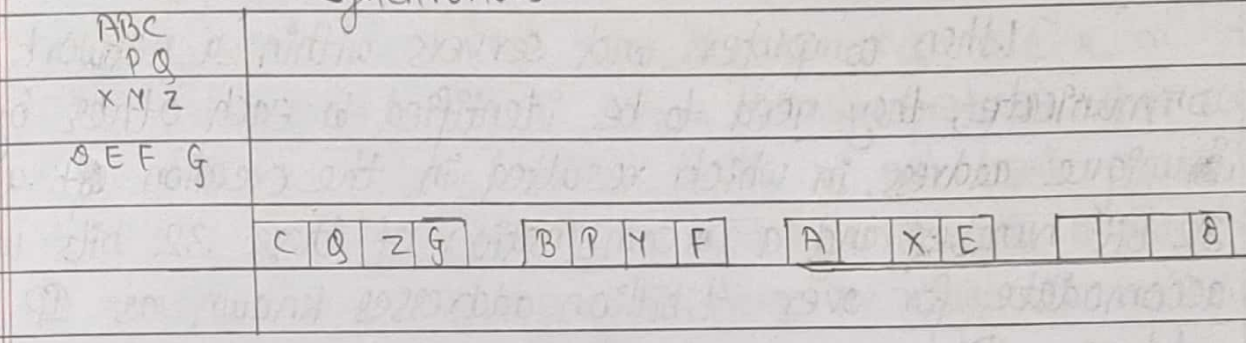
2) Time Division Multiplexing (TDM):-

In TDM, multiple transmission can occupy a single link by sub dividing them and interleaving the portion. TDM can be implemented in two ways:

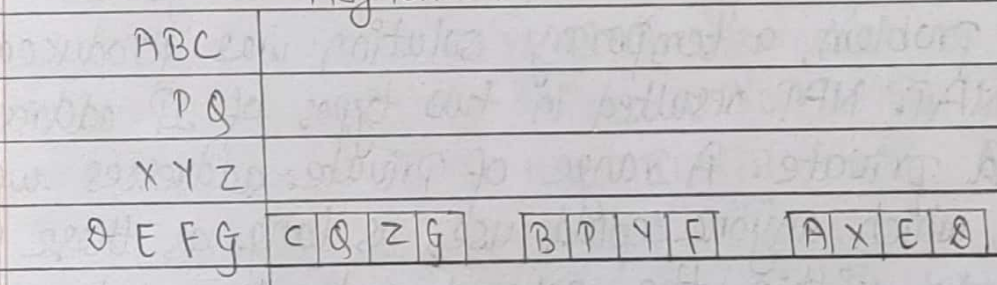
a) Synchronous TDM (khali data pani pathauxa)

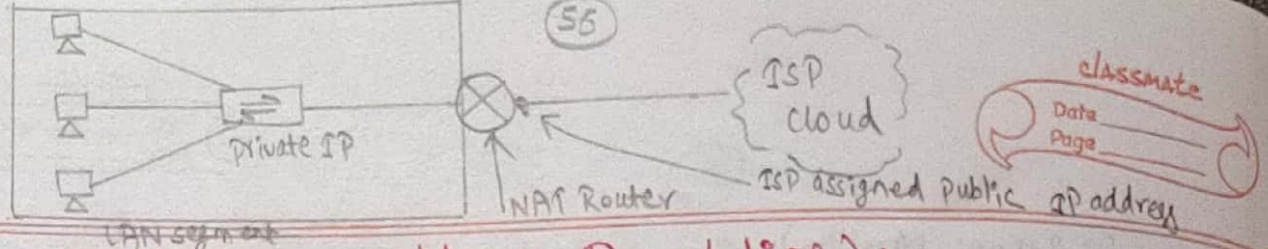
b) Asynchronous TDM (khali data pathaudaina)

Synchronous



Asynchronous





NAT (Network Address Translation):-

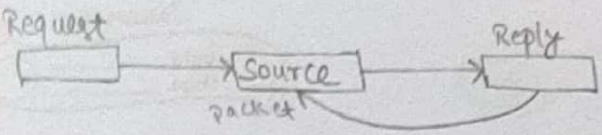
The process of conversion of private IP address to public internet address is called NAT.

→ The IPV4 address have limited address space. So, to save IP address, each LAN segments are addressed with IP address. Those private IP address need to be converted to public IP address to reach to the Internet. The conversion is done by the edge router connected to the service provider generally.

Primarily NAT was introduced to the world of networking due to the lack of IP addresses, or looking at it from another view, due to the vast amount of growing IT technology relying on IP addresses. To add to this, NAT adds a layer of security by hiding devices from the outside world.

When computers and servers within a network communicate, they need to be identified to each other by a unique address, in which resulted in the creation of a 32 bit number and a combination of these 32 bits would accomodate for over 4 billion addresses known as IP address. This was named IPv4, and although over 4 billion addresses sounds a lot, it really is not considering how fast the world of computers can internet has grown. To avoid this problem, a temporary solution was produced known as NAT. NAT resulted in two types of IP addresses; public and private. A range of private addresses were introduced, which anyone could use, as long as these were kept private within the network and not routed on the internet.

When the host from the internal network within an internal IP address does need to communicate outside its private network, it would use the public IP address on the network's gateway to identify itself to the rest of the world, this translation of converting a private IP address to public is done by NAT.



ICMP (Internet Control Message Protocol):

ICMP is a reporting protocol. Network devices like routers used to generate error messages (messages to the source IP address when the network problems prevents delivery of IP packets. ICMP creates and sends message to the source IP address indicating that a gateway to the internet, service or host cannot be reached for packet delivery. Any IP network device has the capability to send, receive or process ICMP messages. ICMP is not a transfer protocol that sends data between systems. While ICMP is not used regularly in end user applications, it is used by network administrators to troubleshoot internet connections in diagnostic utilities including Ping and tracert.

One of the main protocol of the Internet Protocol suite, ICMP is used by routers, intermediatory devices or host to communicate error information or updates to other routers, intermediatory devices or host. The widely used IPV4 and the newer IPV6 use ICMPV4 and ICMPV6 respectively. ICMP messages are transmitted as datagrams and consists of an IP header that encapsulates the ICMP data. ICMP data also contain the entire IP header from the original message, show the end system knows which packet failed.

IP address class:

Internet Protocol contains several classes of IP addresses to be used efficiently in various situations as per the requirement of host. Broadly IPV4 addressing system is divided into 5 class of IP addresses. All the 5 classes are

identified by the first octet of IP address.

Class-A address:

The first bit of first octet is always set to zero. Thus the first octet ranges from 1-127.

Class-B address:

An IP address which belongs to class B ranges from 128-191.

Class-C address:

An IP address which belongs to class C ranges from 192-223.

Class-D address:

An IP address which belongs to class D ranges from 224-239.

Class-E address:

An IP address which ~~ranges~~ belongs to class E ranges from 240-255.

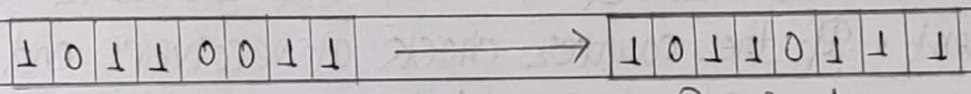
Class A and B are used for public network, class C is used for private network, class D is used for multicasting and class E is used for experimental purpose.

Error detection & Error Correction Techniques:

There are many reasons which may help data to get corrupted during transmission. Most of the applications would not function expectedly if they receive erroneous data. Application such as voice and video may not be that affected and with some errors they may still function well. Datalink layer uses some error control mechanism to ensure that frames are transmitted with certain level of accuracy. But to understand how error is controlled, it is essential to know what type of errors may occur.

Types of errors:

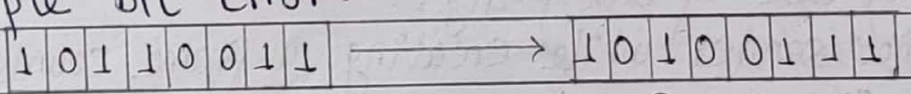
1) Single bit Error:-



Sent Received

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

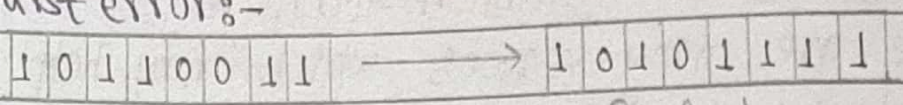
11) Multiple bit Error:-



Sent Received

Frame is received with more than one non-consecutive bit in corrupted state.

iii) Burst error:-



Frame contains more than one consecutive bits corrupted.

There are two types of control mechanism.
i) Error detection
ii) Error correction

1) 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's end fails, the bits are considered corrupted.

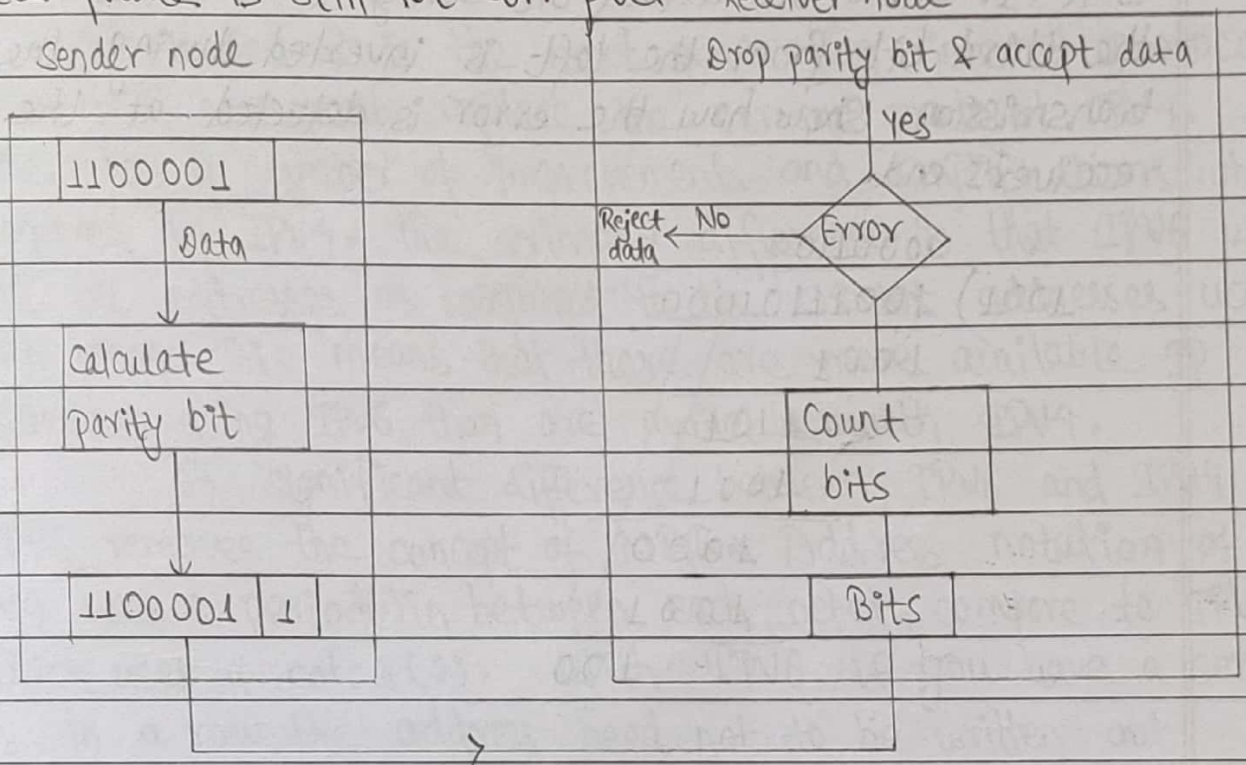
Parity check:-

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

The sender while creating a frame counts the number of 1's in it. For example: if even parity is used and number of 1's is even then one bit with value 0 is added. This way, number of 1's remains even. If the number of 1's 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 counts of 1's is even and even parity is used, the frame is considered to be non-corrupted and is accepted. If the counts of 1's is odd and odd parity is used, the frame is still not corrupted. Receiver node



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 division 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 actual bits.

Example:

A bit stream 10011101 ($x^7+x^4+x^3+x^2+1$) is transmitted using a standard CRC method. The generator polynomial is x^3+1. Show the actual bit string transmitted. Suppose the third bit from the left is inverted during the transmission. Show how the error is detected at the receiver's end.

```
          10001100
     1001 ) 10011101000   (n-1):0 thapne
              1001
               101
               001
               000
               001
                 100
```

Senders: 10011101

Receivers: 10111101 after inverting 3rd bit from left.

```
          10101000
     1001 ) 10111101100
              1001
               011
               001
                001
                001
                 100
```

Since, the remainder is 100 and is not equal to 0, the receiver detects error and can ask for retransmission.

IPV6 :-

IP version-6 is the next generation internet protocol which will eventually replace the current protocol IPV4. IPV6 has a number of improvements and simplifications when compared to IPV4. The primary difference is that IPV6 uses 128 bit addresses as compared to the 32-bit addresses used with IPV4. This means that there are more available IP addresses using IPV6 than are available with IPV4.

A significant difference between IPV6 and IPV4 is IPV6 removes the concept of NAT. Address notation of IPV4 uses a period(.) in between each octet, compare to IPV6 which uses a colon(:). With IPV6 if you have a series 0s in a row, the address need not to be written out completely. You can use a double colon (::) to represent that series of zeros.

Eg:-

2001 : odb8 : 0000 : 130F : 0000 : 6F00 : 087C : 140B

2001 : odb8 :: 130F :: 6F00 : 087C : 140B

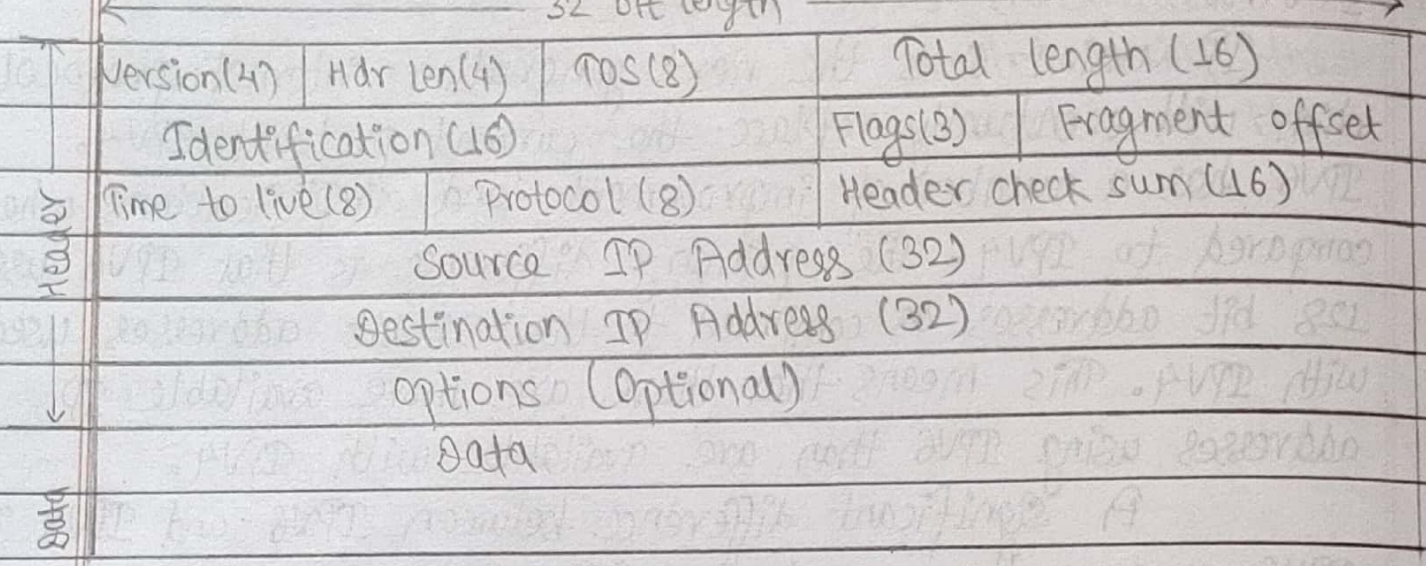
Features:

1. Simplier header :- less no. of fields, no checksum calculation
2. Dual stack:-
   - Two IPV6 address can be assigned
   - One link local address assigned automatically
   - 2nd is global unicast address that should be assigned by n/w admin
3. Transmission reachness :-
   - Compatible to IPV4.

TOS → Type of service

IP datagram

IP datagram is a representation of data along with its header information.



Version :-

It identifies the version of IP used to generate the datagram. The purpose of this field is to ensure compatibility between devices that may be running different versions of IP. In general, a device running a different version of IP will reject datagrams created by another version.

Header Length :-

Specifies the length of IP header. This includes the length of any optional field if used. The normal value of this field when no options are used is 5×32 bits.

Type of Service (TOS):-

A field designed to carry information to provide quality of service features, such as prioritized

delivery, for IP datagrams. This field is often ignored by current routers but is meant to allow traffic to be prioritized.

Total length:-

The length of the entire datagram including header and data: maximum permitted with 64 KB.

Identification:-

This field contains a 16-bit value that is common to each of the fragments belonging to the particular message; for datagrams originally sent unfragmented: it is still filled in, so it can be used if the datagram must be fragmented by a router during delivery. This field is used by the recipient to reassemble messages without accidently mixing fragments from different messages. This is needed because fragments may arise from multiple messages mixed together.

Flags:-

There are three types of flags: Res. (Reserved is not used), DF (Don't Fragment, when set to 1) and MF (More Fragments, when set to 0). Last fragment is identified by flag 1).

Fragment Offset:-

When fragmentation of message occurs, this field specifies the offset or position in the overall message where the data in this fragments goes.

Time to live (TTL) :-

Specifies how long the datagram is allowed to live on the network, interms of router hops. Each router decrements the value of TTL field (reduces it by 1) prior to transmitting it. If the TTL field drops to 0, the datagram is assumed to have taken too long a route and is discarded.

Protocol (8) :-

Specifies the upper layer protocol used, either TCP or UDP.

Header check sum :-

A check sum computed over the header to provide basic protection against corruption in transmission. At each hop, the device receiving the datagram does the same check sum calculation and on a mismatch, discards the datagram as damaged.

Source IP Address :-

The 32-bit IP address of the originator of the datagram.

Destination IP Address :-

The 32-bit IP address of the intended recipient of the datagram.

Options :-

One or more of options may be included after the standard headers in certain IP datagram. Eg: You can record

the path followed by the datagram.

Data :-

The data to be transmitted in the datagram either an entire higher level message or a fragmented one.

duita IP (device to ra network) to bichma separation garauxa

Subnet Mask :-

The 32-bit IP address contains information about the host and its network. It is very necessary to distinguish both. For this, routers use subnet mask, which is as long as the size of the network address. If the IP address is in binary and is ANDed with its binary subnet mask, the result yields the network address.

IP :	11000000	10101000	00000001	10011000
Subnet :	11111111	11111111	11111111	00000000
	11000000	10101000	00000001	00000000

2.1) Link layer & local area Network:-

Network layer provides a communication service between two host, this communication path comprises a series of communication links, starting at the source host, passing through a series of routers (network devices) and ending at the destination host. As we continue to proceed down the protocol stack, from the network layer to the link layer, we wonder how packets are sent across the individual links that make up the end-to-end communication path.

Data link layer is responsible for converting data stream to signals bit-by-bit and to send that over the underlying hardware. At the receiving end, data link layer picks up data from the hardware which are in the form of electrical signals, assembles them in a recognizable frame format and handsover to upper layer.

Although the basic service of any link layer is to move a datagram from one node to an adjacent node over communication link, the details of the provided service can vary from one link layer protocol to the next. Possible services that can be offered by a link layer protocol include:

1) Framing:- Almost all link layer protocols encapsulates each network layer datagram within a link layer frame before transmission over the link. A frame consists of a data field, in which the network layer datagram is inserted, and number of header fields. The structure of the frame is

specified by the link layer protocol.

2) Link access :- A medium access control protocol specifies the rules by which a frame is transmitted into the link. For point-to-point link that have a single sender at one end of the link and a single receiver at the other end of the link, the MAC protocol is non-existent – the sender can send a frame whenever the link is idle. The more interesting case is when multiple nodes sharing a single broadcast link – the so called multiple access problem. Here the MAC protocol serves to co-ordinate the frame transmission of the many nodes.

3) Reliable delivery :-

When a link layer protocol provides reliable delivery services, it guarantees to move each network layer datagram across the link without error. Recall the certain transport layer protocol (TCP) also provides a reliable delivery service. Similar to a transport layer reliable delivery, a link layer reliable delivery service is often achieved with acknowledgements and retransmission.

4) Flow control :-

The nodes on each side of the link have a limited amount of frame buffering capacity. This is a concerned when a receiving node may receive frames at a rate faster than it can process them. Without flow

control, the receiver's buffer can overflow and frames can get lost. Similar to the transport layer, a link layer protocol can provide flow control inorder to prevent the sending node on one side of a link from over whelming the receiving node on the other side of the link.

5) Error detection :-

The link layer hardware in a receiving node can decide that data is not same as it was send from sender. Because there is no need to forward a datagram that has an error, link layer protocols provide a mechanism to detect such error. This is done by having the transmitting node include error detection bits in the frame, and having the receiving node perform and error check.

6) Error Connection:-

Error correction is similar to error detection, except that a receiver not only detects when error have occured in the frame but also determines where in the frame the errors have occurred and acknowledge it

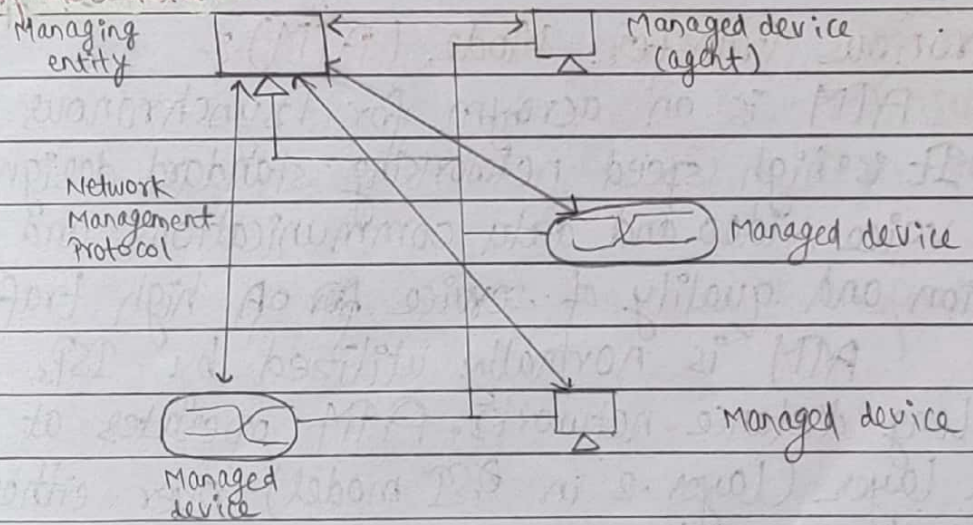
Network Management :-

Network Management includes the deployment, integration and co-ordination of the hardware, software and human elements to monitor, test, poll, configure, analyze, evaluate and control the network and element resources to meet the real time, operational performance, and quality of service requirements at a reasonable cost.

Benefits of Network Management :

- Prevent from failure of network devices.
- Security monitoring
- Host monitoring
- ~~Security monitoring~~
- Traffic monitoring
- Monitoring of rapid changes in routing table.

Infrastructure :-



Managed device (Agent):-
Devices to be monitored / controlled. Example: computers, routers,

Managing Entity:-
An application used by manager to do network management. It controls the network managed devices by analyzing their status.

Network Management Protocols:-
Runs between the managing entity and the managed devices. The managing entity can query the status of managed devices and take actions at the devices via its agent. Example: SNMP (Simple Network Management Protocol).

Asynchronous Transfer Mode (ATM):-

ATM is an acronym for Asynchronous Transfer Mode. It is a high speed networking standard designed to support voice, video and data communications and to improve utilization and quality of service on high traffic networks.

ATM is normally utilized by ISPs on their private long distance networks. ATM operates at the data link layer (layer-2 in OSI model) over either fiber or twisted pair cable.

ATM uses 53 byte (including address header & data) cells. These extremely small packets can be processed through

an ATM switch fast enough to maintain data transfer speeds. The technology was designed for the high speed transmission of all forms of media from basic graphics to full motion video. Because the cells are so small, ATM equipment can transmit large amount of data over a single connection while ensuring that no single transmission takes up all the bandwidth. It also allows ISP to assign limited bandwidth to each customer. While this may seem like a downside for the customer, it actually improves the efficiency of the ISPs internet connection, causing the overall speed of the connection to be faster for everybody.

Each cell is processed at their own time. When one is finished, the procedure then calls for the next cell to process. This is why it is called asynchronous; none of them go off at the same time relative to the other cells. Without routing and with fixed size cells, network can much more easily manage bandwidth under ATM than other technology like Ethernet. The high cost of ATM relative to ethernet is one factor that has limited its adaption to the backbone and other high performance specialized networks.

- Making packets of fixed size and then transferring those fixed sized packets.
- Transfers data using VPI / VCI.
- It has different layer of mechanism,
- AAL is the main field in ATM (Adaptation layer)

Multimedia Networking:

In recent years, there has been an explosive growth of new applications on the internet like streaming video, teleconferencing, interactive games, distance learning and so on. Those multimedia networking applications are referred as continuous media applications and require services different from those for traditional applications like e-mail, web remote logging, etc. They are also different from download and then play applications. Specially, the new application require high quality on the communication latency and the latency variation but may not require high quality on the error rate. One key issue for supporting new multimedia networking applications is how to get the high quality for the communication latency on the best effort internet.

Applications of multimedia networking are:-

a) **Streaming stored audio and video:**

Stored media, the content has been pre-recorded and is stored at the server. So, a user may pause, rewind, or fast forward the multimedia contents.

b) **Streaming live audio and video:**

Applications are similar to traditional radio and television, except that audio/video contents are transmitted on the internet. In these applications, many clients may receive the same audio/video.

c) Real time interactive audio-video:

Applications allow users using audio/video to communicate with each other in real time. Real time interactive audio on the internet is known as Internet phone.

Streaming Audio/Video:-

In these applications, client request audio/video data from servers. Upon client's request, server send the data into a socket connection for transmission. Both TCP and UDP socket connections have been used in practice. The data are segmented and the segments are encapsulated with headers appropriate for audio/video traffic. The real time protocol (protocol that allows a media player to control the transmission of a media stream) is a public domain standard for encapsulating such segments. Audio/video streaming applications usually provide user interactivity which requires a protocol for client-server interaction.

Client request data through a web server. A separate helper application (media player) is required for playing out the audio/video. Well used helper application include real player and media player.

Access audio/video through web server:-

The audio/video files can be delivered by a web server or by an audio/video streaming server. When an audio file is delivered by a web server, the file is treated as an ordinary object in the server's file system like html and image files. To get the file, a client

establishes a TCP connection with the server and sends an http request for the object. On receiving the request the web server encapsulates the audio file in a http response message and sends the message back to the TCP connections. It is more complicated for the video case because usually the sounds and images are stored in two different ways. In this case, a client sends two http request over two separate TCP connections and the server sends two responses, one for sound and other for images to the client. It is upto the client to synchronize two streams.

Sending multimedia from a streaming server to helper application :-

Audio/video files can be delivered by a streaming server to a media player. With streaming server, audio/video file can be transmitted over TCP as well as UDP, UDP is recommended which has much smaller end-to-end delay than TCP.

LAN Address & Address Resolution Protocol :-

LAN address also known as physical address (MAC address) of a device is unique and that address allocation is administered by IEEE. Manufacturers buys portion of LAN address with IEEE to assure uniqueness.

Address Resolution Protocol redirects the data to correct destination in networking using routing table.

Routing table is the collection of information about the MAC address, IP address associated to that MAC address and time to live of that MAC address in a router.

Frame Relay:-

A leased line is a dedicated, point-to-point connection between two routers that pass through a WAN switch, no one else shares that line, there is no frame relay, you (the company) have sole right to all the bandwidth on that line.

Frame Relay is a packet switched WAN technology. The virtual link between your local router and destination router is called a permanent virtual circuit (PVC). What that means is that the frames (data link layer protocol data unit) are relayed from the first frame relay switch that your local router is connected to and the last frame relay switch that the destination router is connected to.

The frame relay between the first frame relay switch and the last frame relay switch is both shared by other customers of the ISP as well as your frames are switched and routed around by the ISP's networking devices until the frame reaches the destination router.

- Layer 1 & Layer 2 protocol.
- Cost effective
- For customer connection, frame relay is used.
- Works on DCE (ISP) / DTE (end-to-end) basement.
- Similar to PPP header format.

Flag | Address | Data | Checksum | Flags |

↳ Multiple fields
DLCI: determines where to go and uses virtual circuit. - is a tag.

Bluetooth :-

Bluetooth is a short range radio technology, which is developed for Personal Area Network (PAL). Bluetooth is a standard developed by a group of electronic manufacturers that allows any sort of electronic equipment. Example:- from computers and cell phones to keyboards and headphones. To make its own connection, without wires, cables or any direct actions from a user. It is an adhoc network (network that does not rely on a pre-existing infrastructure) operable over a small area. Bluetooth wireless technology makes it possible to transmit signals over short distances between different devices and thereby simplify communication and synchronization between devices.

It is a global standard that eliminates wires and cables between both stationary and mobile devices and also facilitates both data and voice communication over the network.

Multiple Access Protocol:-

This is distributed algorithm that determines how nodes shares channel that is i.e. determined when the node can transmit. There are 3 types of multiple access protocol.

1) Channel partitioning Protocol:

a) Time Division Multiple Access (TDMA):-

In TDMA, the bandwidth of channel is divided among various stations on the basis of time. Each station is allocated a time slot during which it can send its data

i.e. each station can transmit its data in its allocated time slot only. Each station must know the beginning of its slot and the location of its slot. TDMA requires synchronization between stations.

b) Frequency Division Multiple Access (FDMA):-

In FDMA, the available bandwidth is divided into various frequency bands. Each station is allocated a band to send its data. This band is reserved for that station at that time. The frequency band of different stations are seperated by small band of unused frequency. These unused frequency bands are called guard bands that prevents station interference.

c) Code Division Multiple Access (CDMA):-

CDMA also called spread spectrum and code division multiplexing, one of the competing transmission technologies for digital mobile phones. The transmitter mixes the packets constituting a message into the digital signal stream in an order determined by pseudo random number sequence that is also known to the intended receiver, which uses it to extract those parts of the signals intended for itself.

2) Random Access Protocol:

a) ALOHA:-

A shared communication system like ALOHA requires a method of handling collisions that occur when two or more system attempt to transmit on the channel at the same time. In the ALOHA system, a node transmits whenever data is available to send. If another node transmits at the same time, a collision occurs and the frames that were transmitted are lost.

ALOHA is a multiple access protocol at the data link layer and purposes how multiple terminals access the medium without interferences or collisions. There are two different types of ALOHA.

i) Pure ALOHA :-

In pure ALOHA, the stations transmit frames whenever they have data to send. In pure ALOHA, whenever any stations transmits a frame, it expects acknowledgement from the receiver. If acknowledgement is not received within specified time, the station assumes that the frame (or acknowledgement) has been destroyed. If the frame is destroyed because of collision the station waits for a random amount of time and send it again. This waiting time must be random otherwise same frames will collide again and again. Therefore, pure ALOHA dictates that when time out period passes, each station must wait for a random amount of time before resending its frame. This randomness will help avoid more collision.

ii) Slotted ALOHA :-

Slotted ALOHA was invented to improve the efficiency of pure ALOHA as chances of collision in pure ALOHA are very high. In slotted ALOHA, the time of the shared channel is divided into discrete interval called slots. The station can send a frame only at the beginning of the slot and only one frame is send in each slot. In slotted ALOHA if any station is not able to place the frame onto the channel at the beginning of the slot that is it misses the time slot then the station has to wait until the beginning of the next time slot.

b) Carrier Sense Multiple Access (CSMA):-

CSMA is a network access method in which devices attached to the network cable listen before transmitting. If the channel is in use devices wait before transmitting. CSMA protocol was developed to overcome the collision problem. The station senses the carrier or channel before transmitting a frame. Even though devices attempt to sense whether the network is in use, there is a good chance that two stations will attempt to access it at the same time. Consider computers C_1, C_2, and C_3 are willing to send data through a channel. At first C_1 transmits data. In the due course of transmission C_2 and C_3 checks the status of the channel at the same time. Both find the channel to be busy so they wait for time t. After time t, both C_2 and C_3 check the channel and find it free, so that they start to

initiate the process of data transmission which can lead to collision.

There are two types of CSMA:

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

CSMA/CD is a protocol in which the station senses the carrier or channel before transmitting frame. If the channel is busy, the station waits. Additional feature in CSMA/CD is that the stations can detect the collision. The station abort their transmission as soon as they detect collision. In CSMA, this feature is not present. The stations continued their transmission even though they find that the collision has occurred. This leads to the wastage of channel time.

However this problem is handled in CSMA/CD, the stations that places its data onto the channel after sensing the channel continues to sense the channel even after the data transmission. If collision is detected, the station aborts its transmission then send its data again.

ii) CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance):

CSMA/CA protocol is used in wireless network because they cannot detect the collision so the only solution is collision avoidance. For example:- despite all the precautions, collision may occur and destroy data. The positive acknowledgment and the time-out timer can help guarantee that receiver has received the frame.

Whenever the channel is found idle, the station

does not transmit immediately. It waits for a period of time called inter-frame spaces. When channel is sensed to be idle, it may be possible that ~~same~~ distant station may have already started transmitting and the signal of that distant station has not yet reached other stations.

3) Taking Turns Protocol:

There are two types of Taking Turns Protocol.

a) Polling protocol:-

The polling protocol requires one of the nodes to be designated as a master node. The master node polls each of the nodes in a round-robin fashion. In particular, the master node first sends a message to node 1, saying that node 1 can transmit upto maximum number of frames. After node 1 transmits, the master node tells node 2, it can transmit maximum number of frames. But it also has a drawbacks like a protocol introduces polling delay i.e. the amount of time required to notify a node that it can transmit

b) Token-passing protocol:-

In this protocol, there is no master node. A small special purpose data known as token is exchanged among the nodes in some fixed order. For example: node 1 might always send the token to node 2, node 2 might send the token to node 3 and node n might always send the token to node 1. When a node receives a token, it holds

onto the token only if it has some frames to transmit otherwise it immediately forwards the token to the next node.

Adaptive Routing & Non-Adaptive Routing :-

Adaptive Routing uses algorithms and routing protocols that read and respond to changes in network topology. Routing protocols that facilitate adaptive routing include intermediate system to intermediate system protocol for large networks such as Internet. The purpose of adaptive routing is to help prevent packet delivery failure, improve network performance and reduce network congestion.

In non-adaptive routing, when a node is unavailable or busy the packet must either wait for node to be available again or the packet will fail to be delivered.

Sliding Window Protocol :-

A sliding window protocol is a feature of packet based data transmission protocols. Sliding window protocol are used where reliable in order delivery of packets is required. Conceptually each portion of the transmission is assigned unique consecutive sequence numbers, and the receiver uses the numbers to place received packets in the correct order. The number of frames are kept in a window and they are acknowledged at once when all packets are received, the receiver sends a signal having information,

from which frame is expecting the data in next window. At receiver, receiver will organize data and acknowledge sender.

Wireless link : IEEE 802.11

Wireless link IEEE 802.11 is a set of media access control (MAC) and physical layer specifications for implementing wireless local area network communication. They are the world's most widely used wireless computer networking standards used in most home and office networks to allow networking devices (laptop, printer, smartphones, etc.) to talk with each other and access the network without physical connection. They are created and maintained by the Institute of Electrical and Electronics Engineers (IEEE) LAN/MAN standard committee.

The base version of the standard was released in 1997.

Congestion Control

Choke packet :

A choke packet is used in network maintainance and quality management to inform a specific node or transmitter that its transmitted traffic is creating congestion over a network. This forces the node or transmitter to reduce its output rate.

Choke packet are used for congestion and flow control over a network. The routers frequently check for

abnormalities over the network by examining factors like buffers, throughput rate. In the event of congestion, routers send choke packets to all the corresponding segments to reduce their data throughput. The source node is addressed directly by the routers forcing it to decrease its sending rate.

Static routing and dynamic routing :-

Static routing does not involve any changes in routing table unless the network administrator changes or modify them manually. Static routing is simple to design and easy to implement as there is no requirement of complex routing protocols. The routing decisions are not made by current topology or traffic because the static routing system cannot react to network changes hence it does not requires extra resources to learn the changes. That is the reason, static routing is considered as inappropriate for large and constantly changing networks.

The default administrative distance for static route is 1, consequently the static routes will only be covered in the routing table when there is the direct connection to that network. Static routes can be considered as an efficient method for a small and simple network that does not change frequently.

Dynamic routing

Dynamic routing is a superior technique which alters the routing information according to the altering network circumstances by examining the arriving routing update messages. When the network change occurs, it send outs a message to the routes to specify that change, then the routes are recalculated and sent as a new routing update message. This messages update the network, enabling the routes to change their routing table correspondingly.

Unlike static routing, it doesnot require manual updation instead its automatic in manner and updates the routing table information periodically relying upon network condition.

	Static Routing	Dynamic Routing
configuration	Manual	Automatic
Routing Table Building	Routing locations are hand-typed.	locations are dynamically filled in table.
Routing algorithms	Doesnot require	Uses complex routing algorithm
Implemented in	Small network	Large network
Link failure	Link failure obstruct rerouting	doesnot affect the rerouting

As - autonomous system.

Intra-As & Inter-As Routing:-

An autonomous system As is a collection of routers whose prefixes of routing policies are under common administrative control. This could be a network service provider, a large company, a university, division of company or a group of companies. The As represents a connected group of one or more blocks of IP addresses, that have been assigned to that organization and provides a single routing policy to systems outside the As.

Routers within an As use an interior protocol, which handles routing between nodes inside the As. Routing within an autonomous system (Intra-As routing) is internal to that As and invisible to those outside it. The As administrator decides what routing algorithm should run within it. To get traffic from a host in one As to a host in another As, the autonomous system need to be connected. An exterior protocol are used as routing protocol that handles routing between autonomous system (Inter-As routing).

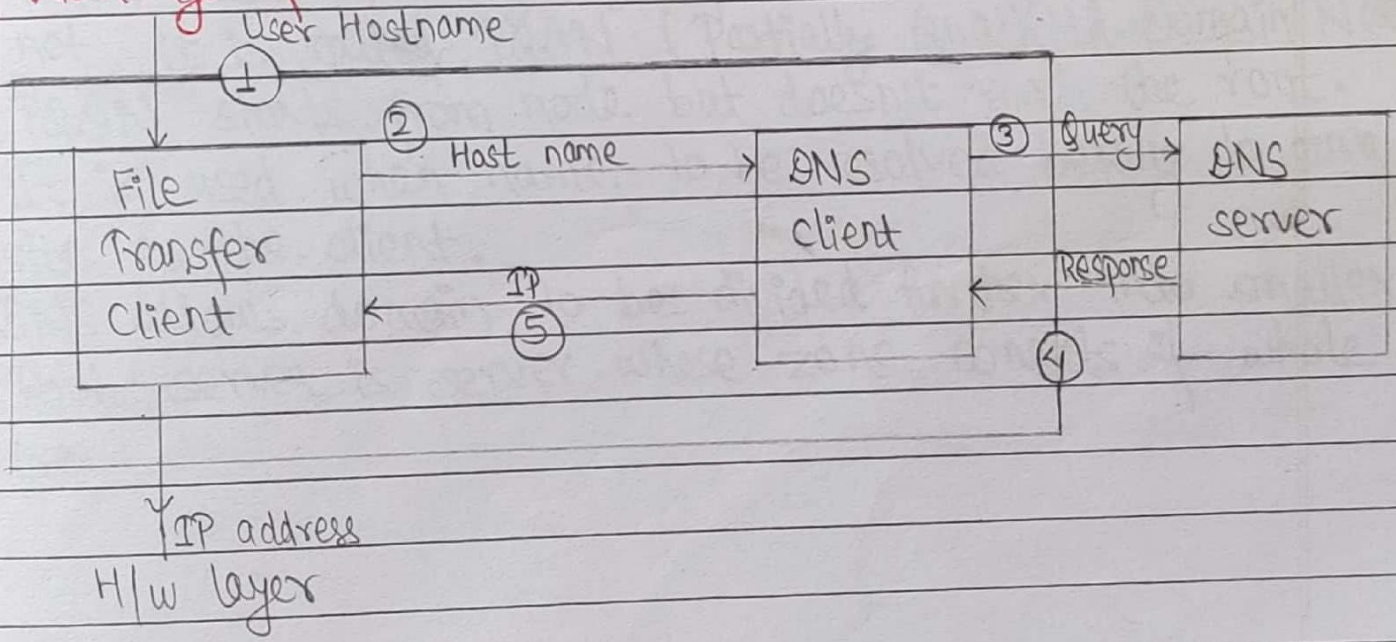
DNS (Domain Name Service):-

- Host name to IP address translation service is provided by DNS.
- Distributed database implemented in hierarchy of name service.
- Application layer protocol.

Why DNS?

- Easier to remember host name than IP address since name has more meaning than 4 byte numbers.
- Application as FTP, HTTP, email all require user to IP destination input hostname.
- Host aliasing :- complicated name has more alias. Example : abc.xyz.media.com ⇒ media.com ⇒ longer is cannonical and shorter is host alias.
- Load balancing on server.

Working of DNS:-



- DNS works by exchanging message between client and server. The mechanism is as below:

1) User provides hostname to file transfer client.
2) File transfer client pass hostname to DNS client.
3) DNS client sends message query to DNS server for IP of file transfer server.
4) DNS server responds with IP.
5) DNS client pass IP to file transfer client.
6) File transfer client now use IP to access file-transfer server.

7) A client application will pass destination hostname to DNS process to get IP address.
8) Application then sits and waits for response to return.
9) DNS message are sent from DNS client to server or between server using UDP port 53 [Request/query are sent with source port (higher number)

Domain Name Space :-

It is a name space that maps each address to a unique name which can be organized in :-

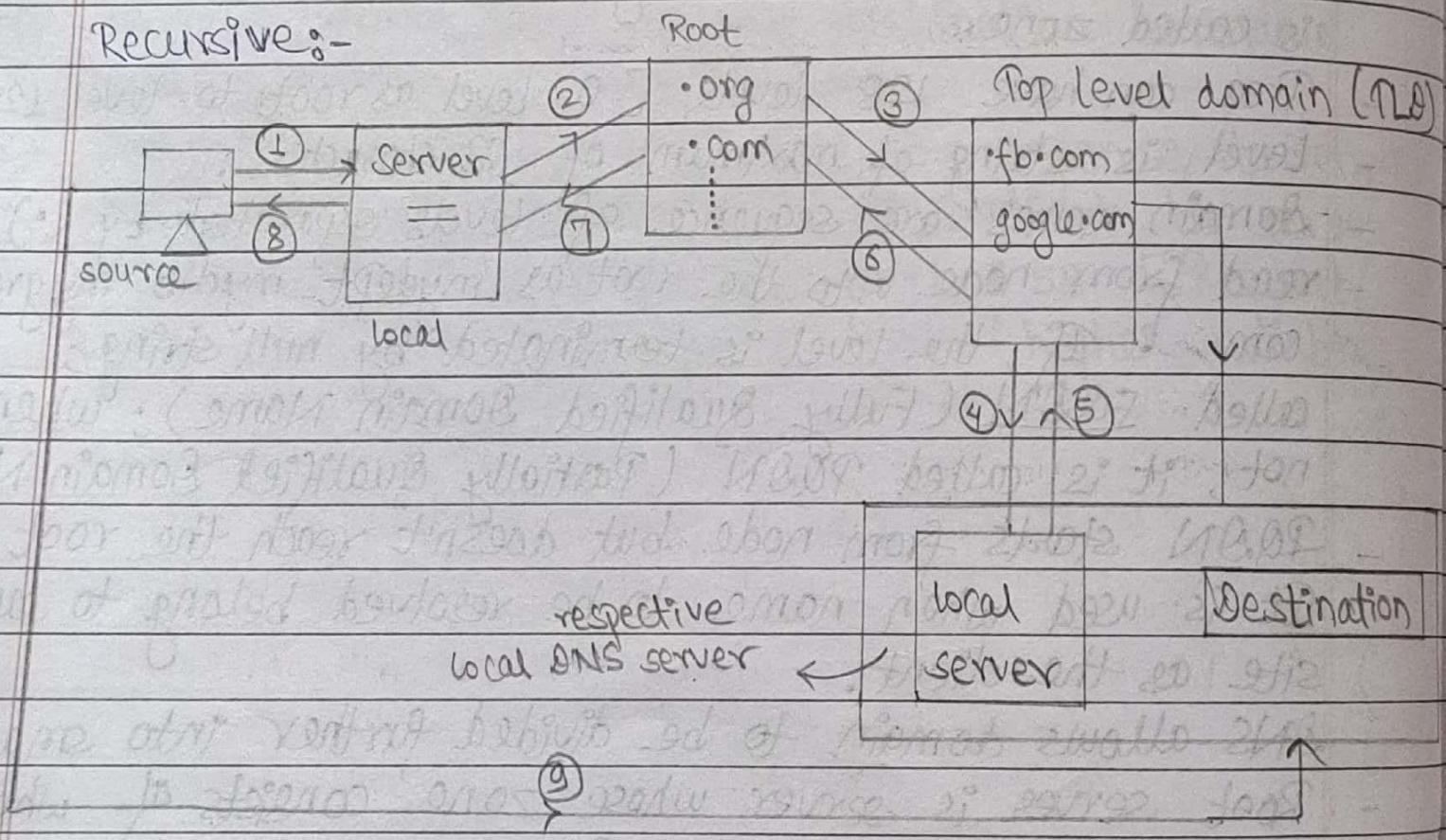
- flat :- sequence of character without structure.
- Hierarchical :- Name is made of several parts. (central authority can define a part that define nature of organization and rest of the name can be given to the organization itself.
- zone :- Domain name hierarchy can't store in single server, so divided into many server. What has authority is called zone.

- Tree can have 128 levels [0 level as root to level 127]
- Level is string of maximum of 63 characters.
- Domain names are sequence of levels separated by (.) read from node upto the root as mydept.mydio.mygroup.com . If the level is terminated by null string; called FQDN (Fully Qualified Domain Name); when not, it is called PQDN (Partially Qualified Domain Name)
- PQDN starts from node but doesn't reach the root. It is used when name to be resolved belong to same site as the client.
- DNS allows domain to be divided further into smaller.
- Root server is server whose zone consists of whole tree.

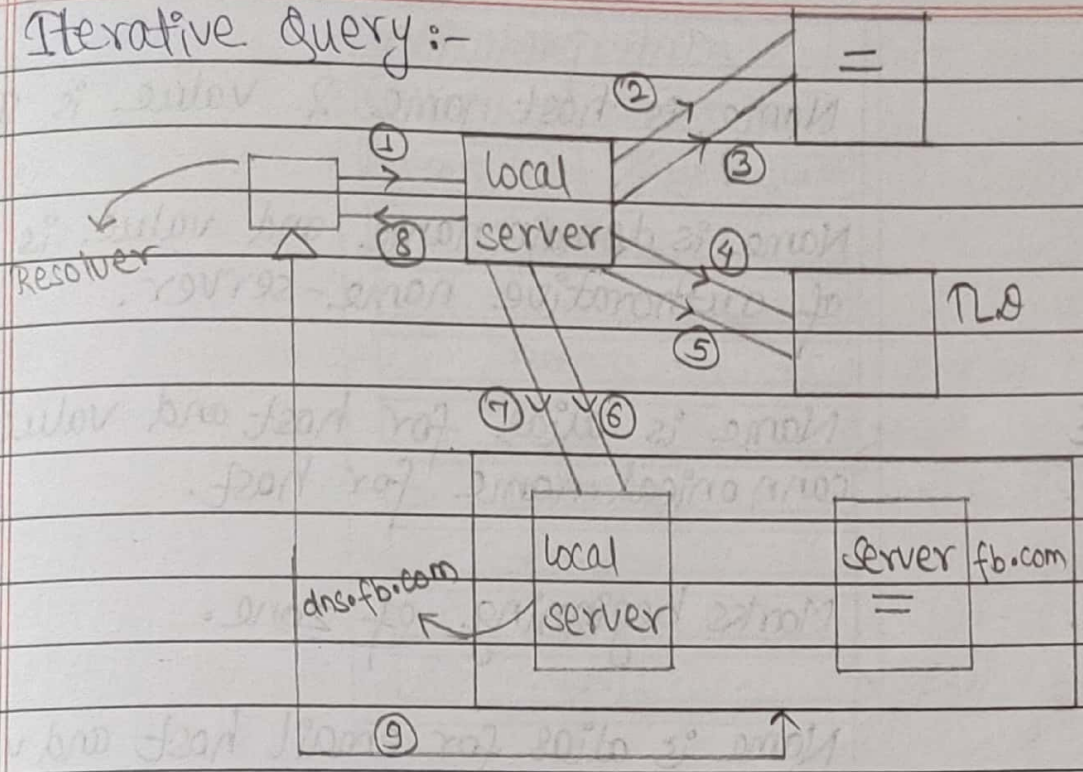
DNS queries / Resolution :-

- A host that needs to map an address to a name or name to an address calls a DNS client called resolver. Resolver access closest DNS server with a mapping request. If server has information it satisfies resolver, otherwise it either refers the resolver to other server or asks other servers to provide information.
- Based on this, resolution can be either recursive or iterative.

Recursive :-



Iterative Query :-



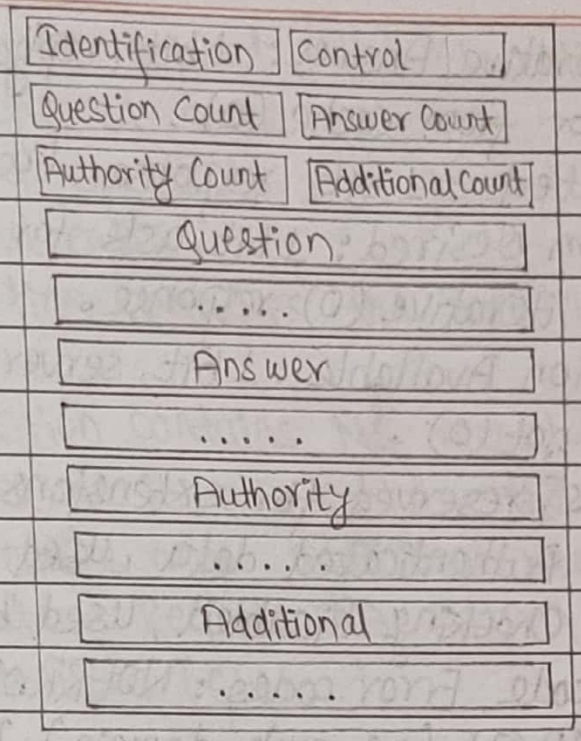
Resource Records :-

- DNS is used in the database called RR (Resource Record). The RR are directly inserted into DNS message.
- RR is 5 tuple structure : [Domain name, type, class, TTL (Time to Leave), value].
- Domain name defines the resource record. It is distributed database.
- Value defines into information kept about the domain name.
- TTL used to indicate when an RR can be removed from DNS cache.
- Class defines type of network.
- Type defines how value should be interrupted.

Type	Interpretation
A	Name is host name & value is IP.
NS	Name is domain name and value is IP of authorative name-server.
CNAME	Name is alias for host and value is cannonical name for host.
SOA	Marks beginning of zone.
MX	Name is alias for email host and value is cannonical name for e-mail server
AAA	IPV6 address

DNS Message:-

The DNS protocol uses a common message format for all exchanges between client and servers. The DNS messages are encapsulated over UDP or TCP using the "well-known port number" 53. DNS uses UDP for message smaller than 512 bytes (common requests and responses). DNS uses TCP for bigger exchange (i.e. zone transfer).



The first 6 fields are 16-bits long, other fields are variable length. Maximum size for a DNS label is 64 Bytes, for a DNS name 255 bytes, for a DNS RDATA value 65535 bytes.

- Identification field is used to match up replies and requests.
- Control field contains

QR	Opcode	AA	TC	RD	RA	Z	AD	CD	RCODE

  - QR : 1 bit, request (0) or response (1)
  - Opcode : 4 bits, request type
    - QUERY : Standard request
    - IQUERY : Inverse request (obsoleted by RFC3425)
    - STATUS : Server status query
    - NOTIFY : Database update notification (RFC1996)
    - UPDATE : Dynamic database update (RFC2136)

- AA : Authorative Answer : 1 bit, reply from authorative (1) or from cache (0).
- TC : Truncated : 1 bit, response too large for UDP (1).
- RD : Recursion Desired : 1 bit, ask for recursive (1) or iterative (0) response.
- RA : Recursion Available : 1 bit, server manages recursive (1) or not (0).
- 1 bit zeros, reserved for extensions
- 1 bit AD Authenticated data, used by DNSSEC
- 1 bit CD Checking Disabled, used by DNSSEC
- 4 bits Rcode, Error codes : NOERROR, SERVFAIL, NXDOMAIN (no such domain), REFUSED ...

- ... count fields give the number of entry in each following sections :
- the Question section contains incomplete RR { DNSname, TYPE, CLASS }.
- sections Response, Authority, Additional contain complete RR.
  { DNSname, TYPE, CLASS, TTL, (RDATA_LENGTH), RDATA }

TYPE, CLASS and RDATA_LENGTH are 2-bytes long, TTL is 4-bytes long, DNSname follows some specific coding rules with compression.

Depending upon request, the 4 sections contain various RR, some required, some optional....

- Question count equals to 1 in general, but could be 0 or >1 in very special cases.
- Response section contains the matching RR set with respect to the question.
- Authority section contains NS record for Authorative zone servers. Sometime it also contains the SOA record.
- Additional contains any additional useful information. For instance Address Records (A, AAAA) for host names used in previous sections (Glue...).

1. Define Protocol. Why do we need layered protocol architecture? Discuss each layer of TCP/IP protocol architecture in detail.

→ Protocol is the rule that should be followed by communicating devices. It defines the way to generate data, convert it into signals, forward it, check error, check medium, etc.

Layering is the organization of programming into separate functional components that interact in some sequential and hierarchical way, with each layer usually having an interface only to the layer above it and the layer below it.

Communication programs are often layered. The reference model for communication programs, OSI is a layered set of protocols in which two multilayered programs, one at either end of a communication exchange, use an identical set of the layers. In the OSI model, each multilayer program contains seven layers, each reflecting different functions that has to be performed in order for program-to-program communication to take place between computers.

TCP/IP is an example of a two layer (TCP and IP) set of programs that provide transport and network address functions for Internet communication. A set of TCP/IP and other layered protocols is sometimes called as protocol stack/suite.

Need of layering architecture :-

1) Reduces complexity :-
It breaks network communication process into smaller and simpler components, thus aiding component development, design, and troubleshooting.

2) Standardizes interfaces :-
It standardizes network components to allow multiple vendor development and support.

3) Facilitates modular engineering :-
It allows different types of network hardware and software to communicate with each other.

4) Encrypt data for security purposes :-
Decryption and encryption services are also available for security purposes. Expansion and compression of message is simplified to ensure it travels from one system to another efficiently.

5) Simplifies teaching and learning :-
It breaks network communication into smaller components to make learning easier. Provides a teaching tool to help network administrators understand the communication process used between networking components.

6) Accelerates Evolution :-

It provides for effective updates and improvements to individual components without affecting other components or having to rewrite the entire protocol.

TCP/IP has a network model which is based on a four-layer reference model as:

I) Application layer :-
- This is the top layer of TCP/IP protocol.
- It includes applications or processes that use transport layer protocols to deliver the data to destination computers.
- At each layer there are certain protocol option to carry out the task designated to that particular layer.
- Some applications of this layer are : HTTP, FTP, SMTP, etc.

II) Transport layer :-
- This layer provides backbone to data flow between two hosts.
- This layer receives data from the application layer above it.
- The two most commonly used protocols in this layer are TCP and UDP.
- TCP is used where a reliable connection is required while UDP is used in case of unreliable connections.

III) Internet layer:-
- It is the second layer of TCP/IP model.
- The internet layer pack data into data packets known as IP datagrams, which contains source and destination address information.
- It is used to forward the datagrams between hosts and networks.
- It is also responsible for routing of IP datagrams.
- Packet switching network depending upon a connectionless internetwork layer is known as internet layer.

IV) Network Access layer:-
- It is the first layer of TCP/IP model.
- It defines details of how data is physically sent through the network, including how bits are electrically signed optically or
- The protocols included in this layer are: Ethernet, Token Ring, FDDI, X.25, frame relay.

Application	Telnet, FTP, DHCP, SMTP, HTTP	Message
Transport	TCP, UDP	Segment port addressing, process to process.
Network	IGMP, ICMP, IP, ARP, RARP	Packet logical address host to host node to node.
Data link		Frames physical address
Physical		bits

Fig:- TCP/IP

2. What is routing? Discuss link state routing algorithm in detail.

→ Routing is one of the important function of network layer.

- It is the process of creating routing table, checking routing table for forwarding packets, taking the best decision to forward the packet through certain routers and finally forwarding packets through that router.
- Forwarding is the process of sending the packet from one host to another.

- Link state routing initially synchronizes with all the routing information of network.
- It then sends updates about routing information (to all routers) when there is some change in network or link state.
- Link state routing computers optimal path using Dijkstra's algorithm.
- It uses bandwidth and delay as its metric cost.
- It consumes less bandwidth and there will be less traffic.
- It is less CPU intensive and maintains three tables viz. routing table, topology table and neighbour table.

a) Routing Table:-
This table stores optimal path from source to destination obtained from Dijkstra's algorithm by using some link cost like bandwidth and delay.

b) Topology Table:-
This table stores map of all links. If optimal path is down then the path in this table is used.

c) Neighbour Table:-
This table contains list of all neighbour routers.

What is transmission media? Discuss each transmission media in detail.

Ans:- Transmission media is defined as the channel to propagate data. It is of two types:
i) Guided media and
ii) Unguided media.

1) Guided media:-
- The waves are guided along a physical path. Eg: phone-lines, twisted pair cables, co-axial cables, optical fibres.
- Signals are confined within the wire and do not propagate outside of wire.
- It is further classified into:-
a) Twisted pair
b) Coaxial cables
c) Fibre optics

a) Twisted pair cables:-

- Twisted pair cable consists of insulated pair of copper wire attached together.
- The twisting of cable is insulated from outer shield.
- The twisting of copper wire helps to reduce noise like cross.
- It is very cheap and common.
- Shielded twisted pair cable has additional shield to prevent.

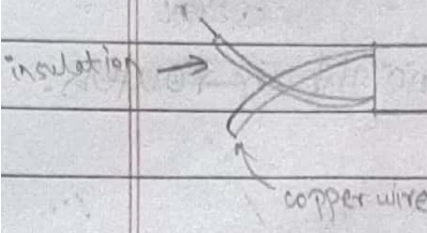


Fig:- UTP

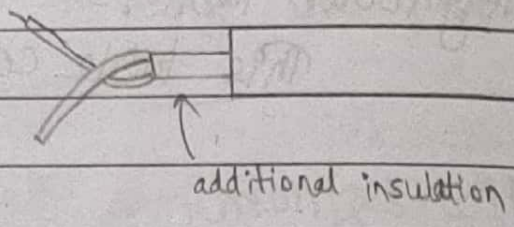


Fig:- STP

b) Coaxial cable:-

- Coaxial cable consists of one copper wire which is insulated by plastic and covered by metallic shield and outer shield as shown in the figure.

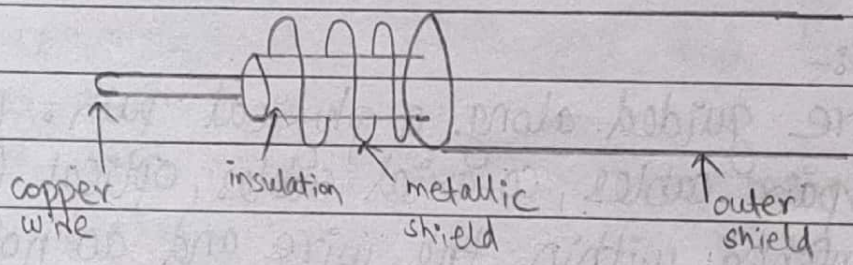


Fig:- Coaxial cable

- Coaxial cable has higher bandwidth than twisted pair cable and is less affected by outer noise.

- It is more expensive than twisted pair cable.
- BNC is jack used for connecting this cable.
- Thicknet has more diameter than thinnet.
- Thinnet supports higher bandwidth and can be used for long distance. But thicknet is less flexible than thinnet and difficult to work with.
- It is mainly used for television cable network and also for LAN networks.

c) Optical fibre :-

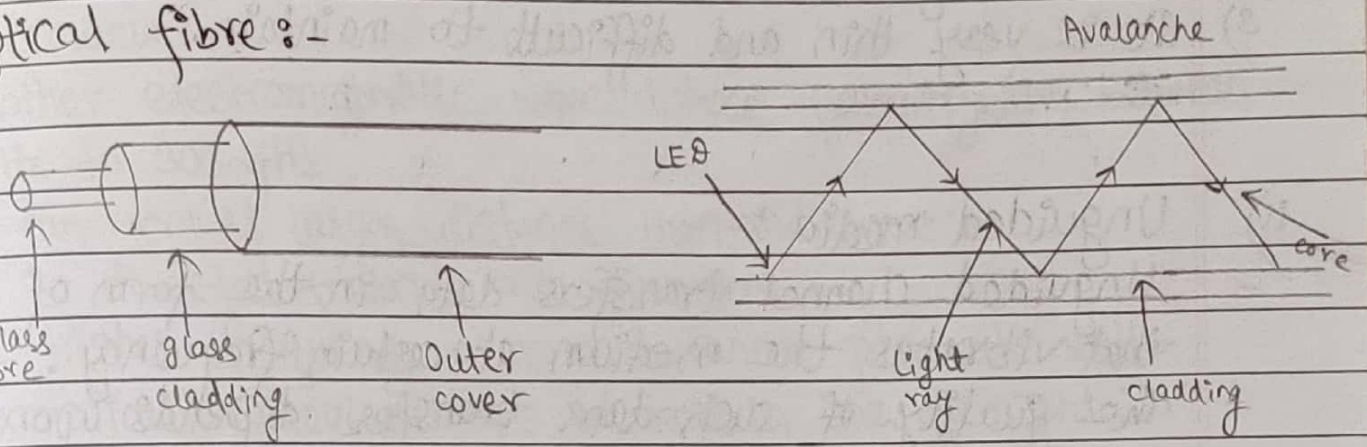


Fig :- Data Transfer

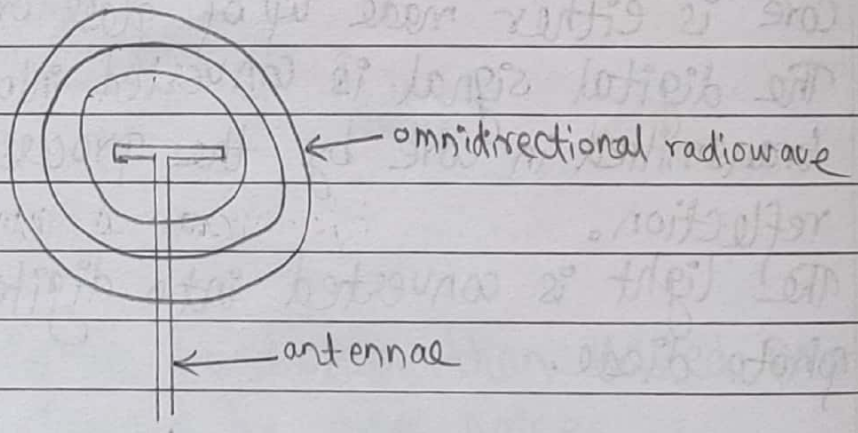
- Optical fibre consists of core glass, glass cladding and outer cover.
- The density of core is lesser than density of cladding.
- Core is either made up of glass or plastic.
- The digital signal is converted into light ray and is transmitted in core by the process of total internal reflection.
- The light is converted into digital signal by avalanche photo diode.

Advantages:-
1) Highest bandwidth upto 100 gps and fastest data rate.
2) Immune to outer noise like interference or cross talk.
3) Data attenuation is very less.
4) More secured.

Disadvantages:-
1) Unidirectional data transfer
2) Cost is high
3) It is very thin and difficult to maintain.

ii) Unguided media:-
- Unguided channel transfers data in the form of wave that vibrates the medium at certain frequency.
- The quality of such data transfer depends upon antennae being used for sending and receiving signal.
- Its data transfer rate is lesser than guided media and less secured.

a) Radiowave:-



- Radiowave is a type of electromagnetic wave whose frequency lies between 3KHz to 1GHz.
- Can penetrate wall.
- Omnidirectional in nature. So, it can broadcast in all directions.
- Sender and receiver must not be kept in line of sight.
- Can't travel long distance. In face, distance covered by radio wave depends upon height of antennae.
- Used in FM, AM, mobile communication, etc.

b) Microwave:-
- Another electromagnetic wave whose frequency lies between 1GHz to 300 GHz.
- It can travel larger distance than radiowave.
- It is directed towards one direction.
- The higher frequency microwave cannot penetrate wall.
- Communication devices must be kept in line of sight.
- Used in satellite, mobile, etc.

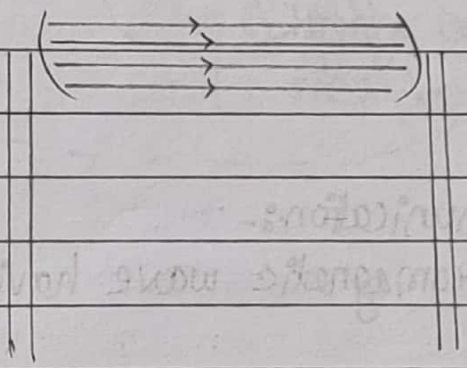
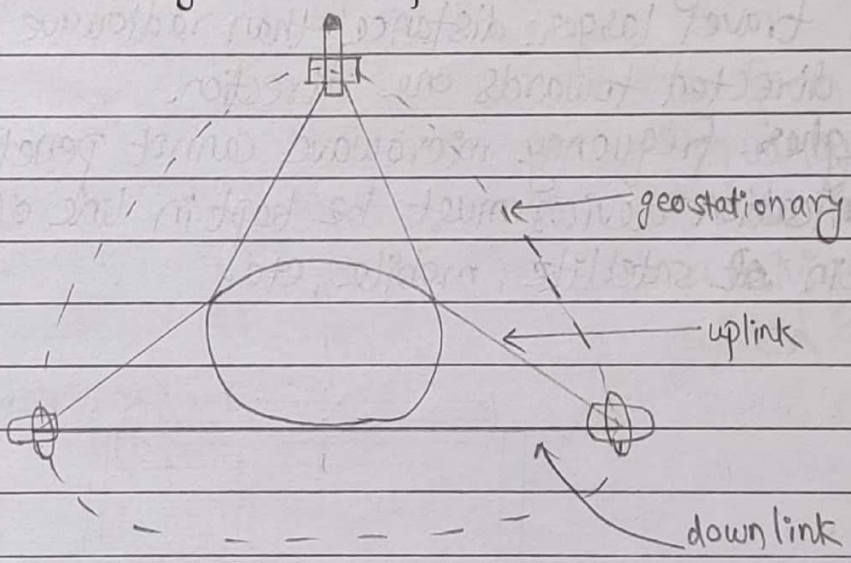


Fig:- Microwave communication

c) Satellite communication :-
- In satellite communication, number of satellites are kept at some height from earth.
- These satellites revolve the earth.
- Satellites contains no. of transponder which can receive and send microwave from or to earth station.
- The transponder receive signals in one frequency which is called uplink and send signal to another frequency called down link.
- The satellite is generally kept at geostationary orbit of earth which is at 35700 height from earth so that satellite remains stationary with respect to earth.



d) Infrared communication :-
- Also an electromagnetic wave having frequency 300 GHz to 400 THz.
- Used for short distance communication
- Communication must be in line of sight.
- It can't penetrate waves or other obstacles.
- Used in remote control, mobiles, etc.

Difference between guided and unguided media:

Unguided media	Guided media
1. Physical paths are not used for transmission so called wireless.	1) Physical paths are used for the transmission.
2. It is mainly used for broadcasting purposes.	2) It is mainly suited for point to point line configuration.
3. The signal propagates in the form of electromagnetic waves.	3) The signal propagates in the form of voltage, currents or photons.
4. Eg: Microwaves or Radio links.	4) Eg: Twisted pairs, coaxial cables, optical fibres.
5. Data transfer rate is less compared to guided media.	5) Highest bandwidth upto 100 gbps and high data rate.
6. It is less secured.	6) Highly secured than unguided media.

Transport layer:-

- Transport layer is the fourth layer of OSI model. It generally provides services to the upper layer (Application layer).
- The services of transport layer are:-

1. Segmentation:-
- The segmentation is the process of chunking of the message according to the network capacity to transfer from source to destination.
- The segmented / chunked message are then encapsulated with the related layer (transport layer) header.
Segment ⇒ chunked message in the header.

2. Port Addressing:-
- Port is the 16-bit value assigned uniquely to each of the protocols (normally application protocols).
0 to 1024 ports are well known ports and above than that are temporary port [used / defined manually]
Eg: HTTP use port no. 80
HTTPs use port no. 443
SSH use port no. 22
FTP use port no. 20 and 21
SMTP use port no. 25.
POP3 use port no 110, etc.

The combination of IP address with port number is called socket address; normally called socket. The port no. is seperated by (:) colon. Eg: <202.51.07.5:443> ⇒ socket.
↓ from IP address

3. Multiplexing and Demultiplexing :-
- The PDU of different protocol are transferred with the same channel (share the transmission media). It is done with the help of port address.
- The received message / PDU at the receiver are then transfered to correct process / application.

4. Flow control :-
- The transmitting service transmits according to the capability of receiver, so that the receiver doesn't get overwhelmed / swamped. This is done through the process of acknowledgement The transmitter doesnot transmit / retransmit until it gets acknowledgement of reception of segments by receiver.

5. Sequencing :-
- Sequencing is done through the header information that contains sequence number of the segment.

Data link layer :-
- Data link layer is layer-2 of OSI model.
- It is responsible for the point-to-point or node-to-node delivery of PDU.
- Datalink layer encapsulates the PDU coming from upper layer to the frames at transmitter side and assembles the bits into frames that are received at the receiver.
- It also have flow control, error control mechanism.
- DLL is also responsible for the physical addressing also called as MAC-addressing.

- DLL have two sublayers viz. LLC and MAC.
  - LLC : Logical Link Control
  - MAC : Media Access Control

Services of DLL:-

- DLL provides services to upper layer and receives/use services provided by below layer i.e. physical layer.
- DLL provides various services:

i) Framing ii) MAC addressing iii) Error control
iv) Flow control v) Congestion control.

TCP connection establishment : 3 way Handshake.

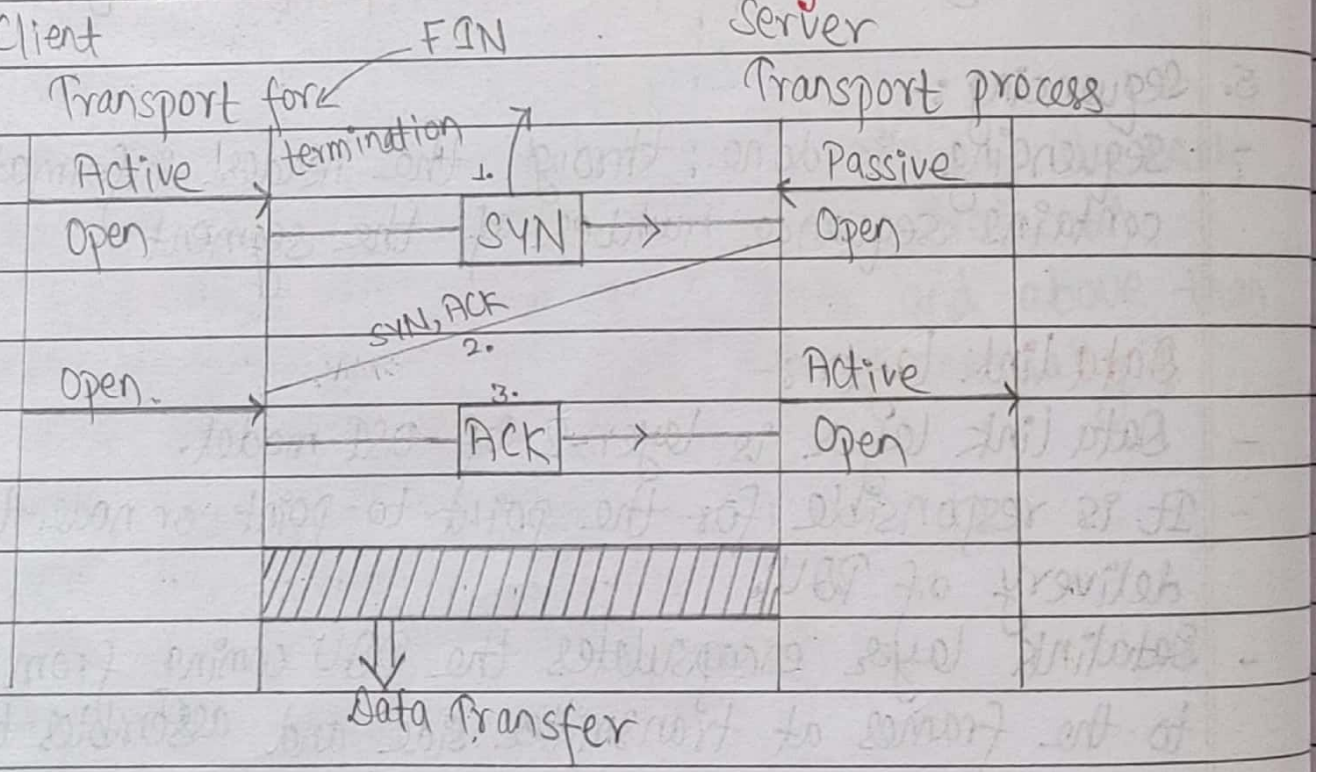


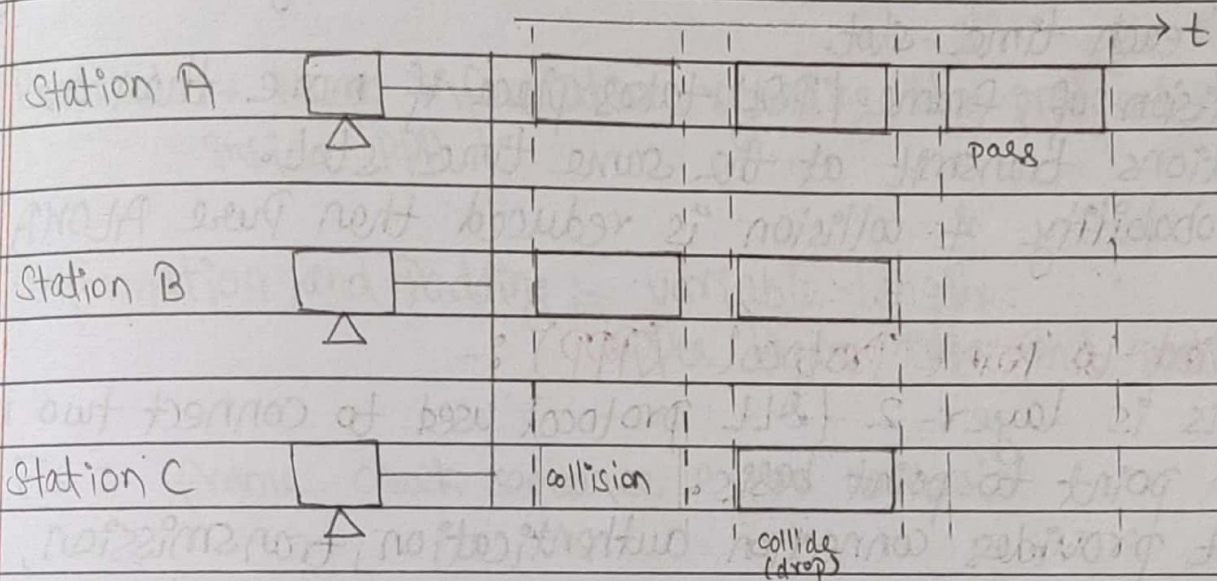
Fig:- 3-way handshake

ALOHA :-

- Channel Access method by a station.
- In aloha if a device wants to transmit, it transmits immediately.
- Based on channel access strategy, there are two types of ALOHA.

i) Pure or unslotted ALOHA
ii) Impure or slotted ALOHA.

i) Pure ALOHA.



- Station can transmit or can access channel on any time it wants.
- If two station transmit at the same time then collision occurs, and frames are destroyed.
- No mechanism to handle collision.
- Maximum chance of collision.

ii) Slotted ALOHA :-

	T_4	T_3	T_2	T_1	
Station A	✓			X	
Station B		X		X	
Station C		X			
					✓

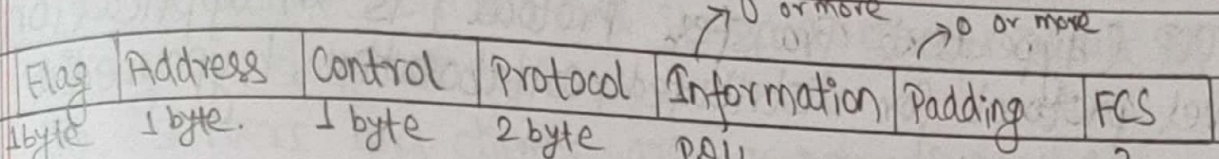
- Stations are allowed to access channels only at the beginning of each time-slot.
- Collision of frame / POU takes place if more than one stations transmit at the same time slot.
- Probability of collision is reduced than Pure ALOHA.

Point to Point Protocol (PPP) :-

- This is layer-2 / DLL protocol used to connect two nodes in point to point basis.
- It provides connection authentication, transmission, encryption and compression.
- It is used over many type of physical network.
- ISP use PPP for customer dial up access to internet.
- Two types :
  - PPPoE :- PPP over Ethernet
  - PPPoA :- PPP over ATM (Asynchronous Transfer Mode)
- Designed to work with number of internet protocols like IP.
- 3 components are Encapsulation, LCP (Link Control Protocol) and NCP (Network Control Protocol).

classmate
Date
Page

PPP Header :-



1. Flag :- Start and end of PPP frame.
   value set is [01111110] 0X7E

2. Address :- Broadcast : 0XFF

3. Control :- 0X03 ; used in HDLC for various control purpose.

4. Protocols :- keeps information regarding the protocol encapsulated inside PPP.

5. Information and Padding :- variable length.
   upper layer data and padding.

6. FCS :- frame check sequence error control.

Discuss HTTP in detail.

→ HTTP (Hypertext Transfer Protocol) is an application-level protocol for distributed, collaborative, hypermedia information systems.

- This is the foundation for data communication for the World Wide Web (www).
- It is generic and stateless protocol which can be used for other purposes as well as using extensions of its request methods, error codes and headers.
- HTTP is a TCP/IP based communication based protocol, that is used to deliver data on world wide web. It uses the default TCP port 80.
- HTTP specification specifies how the servers respon to those requests.

Features of HTTP :-

I) HTTP is connectionless :

- The HTTP client 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.

I) 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.

III) HTTP is stateless:

- HTTP is connectionless and it is a direct result of HTTP being a stateless protocol.
- The servers and clients are aware of each other only during a current request.
- Afterwards, both of them forget about each other.

- HTTP/1.0 uses a new connection for each request/response. It is non-persistent by nature.
- HTTP/1.1 connection may be used for one or more request/response exchange. It is persistent by default and makes persistence of TCP connections.
- HTTP protocol is a request/response protocol based on the client/server architecture.

• HTTP clients:

- The HTTP clients sends a request to the server in the form of 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.

• HTTP server:

- The HTTP server sends 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.

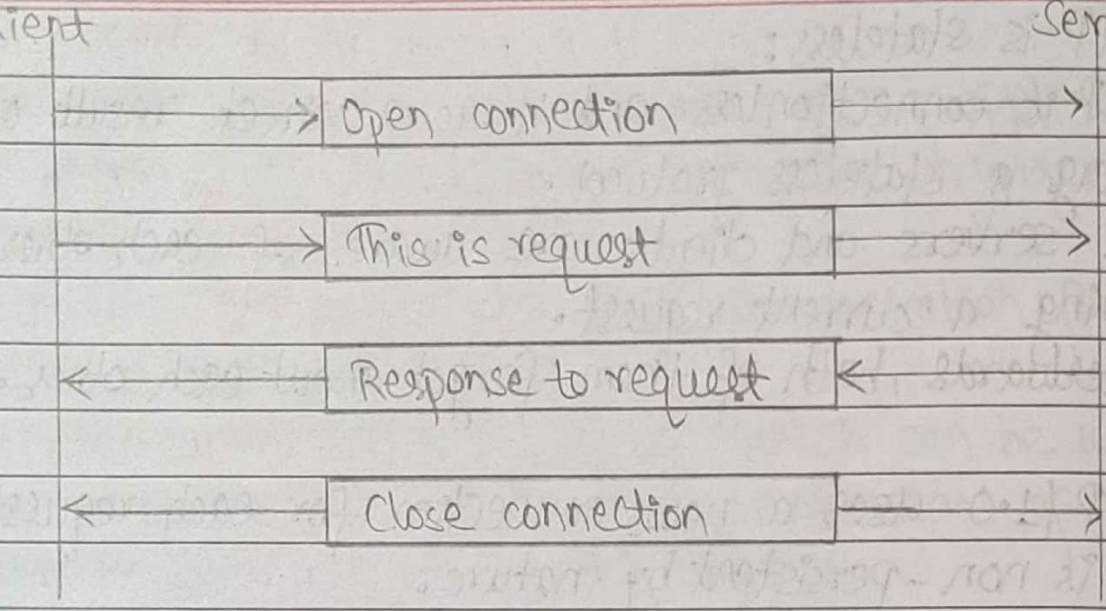


Fig:- HTTP transaction.

Discuss the importance of multiplexing in data communication.

- Multiplexing is a method by which multiple analog message signals or digital data streams are combined into one signal over a shared medium.

The importance of multiplexing in data communication are as follows:-

- Multiplexing shares an expensive resource.
For example :- in communications, the multiplexed signal is transmitted over a communication channel, which may be a physical transmission medium.
- The multiplexing divides the capacity of the low level communication channel into several higher-level logical channels, one for each message signal or data stream to be transferred.
- If no multiplexing is used between the users at two different sites that are distance apart, then separate

communication line would be required, that becomes difficult to manage as well as costly. But, when multiplexing is used, only one line is required. This leads to the reduction in the line cost and also it would be easier to keep track of one line than several lines.

- Multiple number of process, which are running in a host simultaneously, must communicate with multiple process in another host. Thus, transport layer multiplex all these process by assigning different port numbers to these process and send them to IP at sender end.
- However, at the receiver end, transport layer demultiplex the segment by using the distinct port number and hand over the message to respective process.

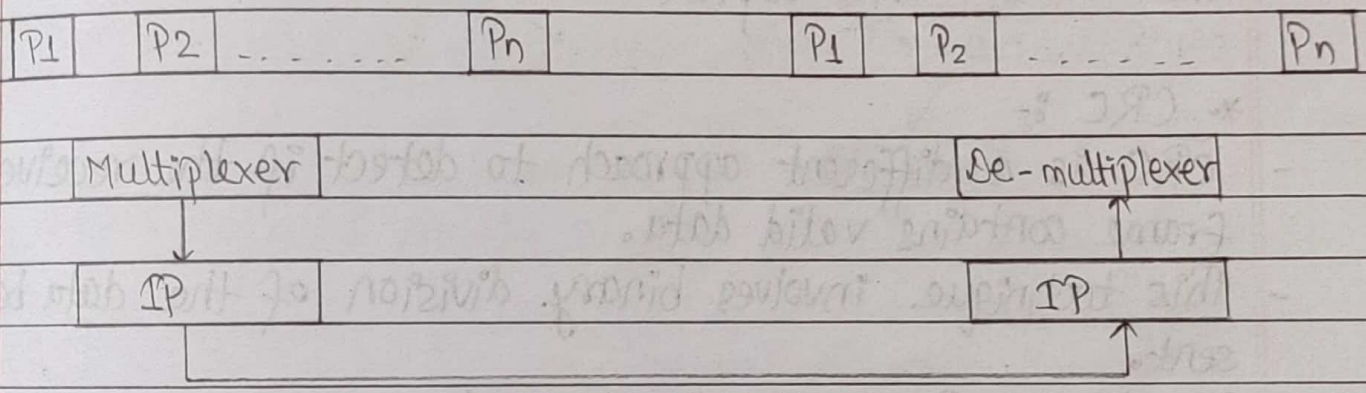


Fig:- Multiplexing - Demultiplexing.

Discuss CRC as an error detection mechanism.

→ There are two possible ways for error control mechanism. They are :-

i) Error detection
ii) Error correction.

i) 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.

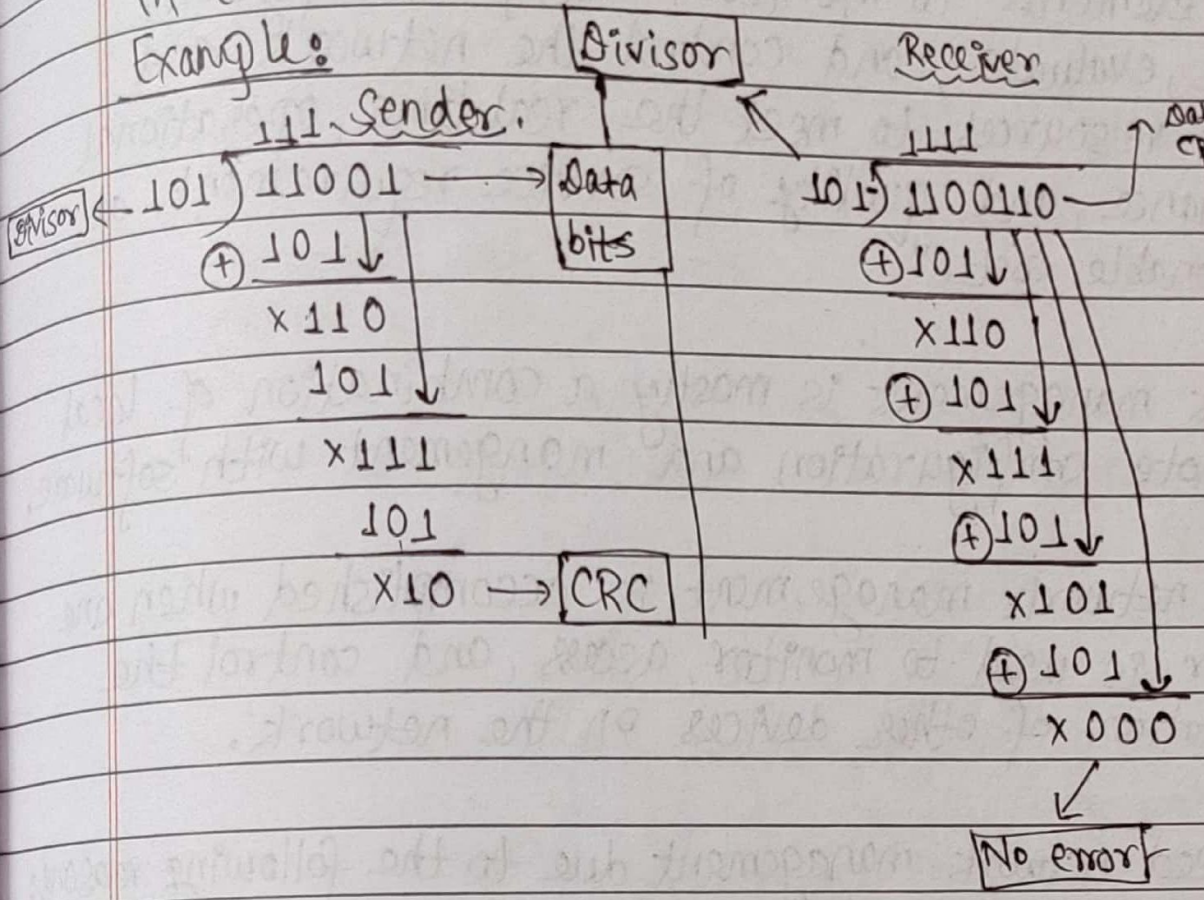
* CRC :-

- CRC is a different approach to detect if the received frame contains valid data.
- This technique involves binary division of the data being sent.
- The division 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 code word.
- The sender transmits data bits as codewords.
- At the other end, the receiver performs division operation

on code words using the same CRC divisor.

- If the remainder contains all zeros the data bits are accepted, otherwise it is considered as some data corruption occurred in transit.

Example:



Why is network management an important task?

→ "Network management includes the deployment, integration and coordination of the hardware, software, and human elements to monitor, test, poll, configure, analyze, evaluate, and control the network and element resources to meet the real time, operational performance, and quality of service requirements at a reasonable cost."

- Network management is mostly a combination of local and remote configuration and mangement with software.
-
- Remote network management is accomplished when one computer is used to monitor, access, and control the configuration of other devices on the network.

We need network management due to the following reasons:

1) It helps in detecting failure of an interface card at a host or router.
2) It hosts monitoring.
3) It helps in monitoring traffic to aid in resource deployment
4) Helps in detecting rapid changes in routing tables.
5) Helps in monitoring for SLAs (Service Level Agreement).
6) Helps in intrusion detections.

Write short notes on DNS.

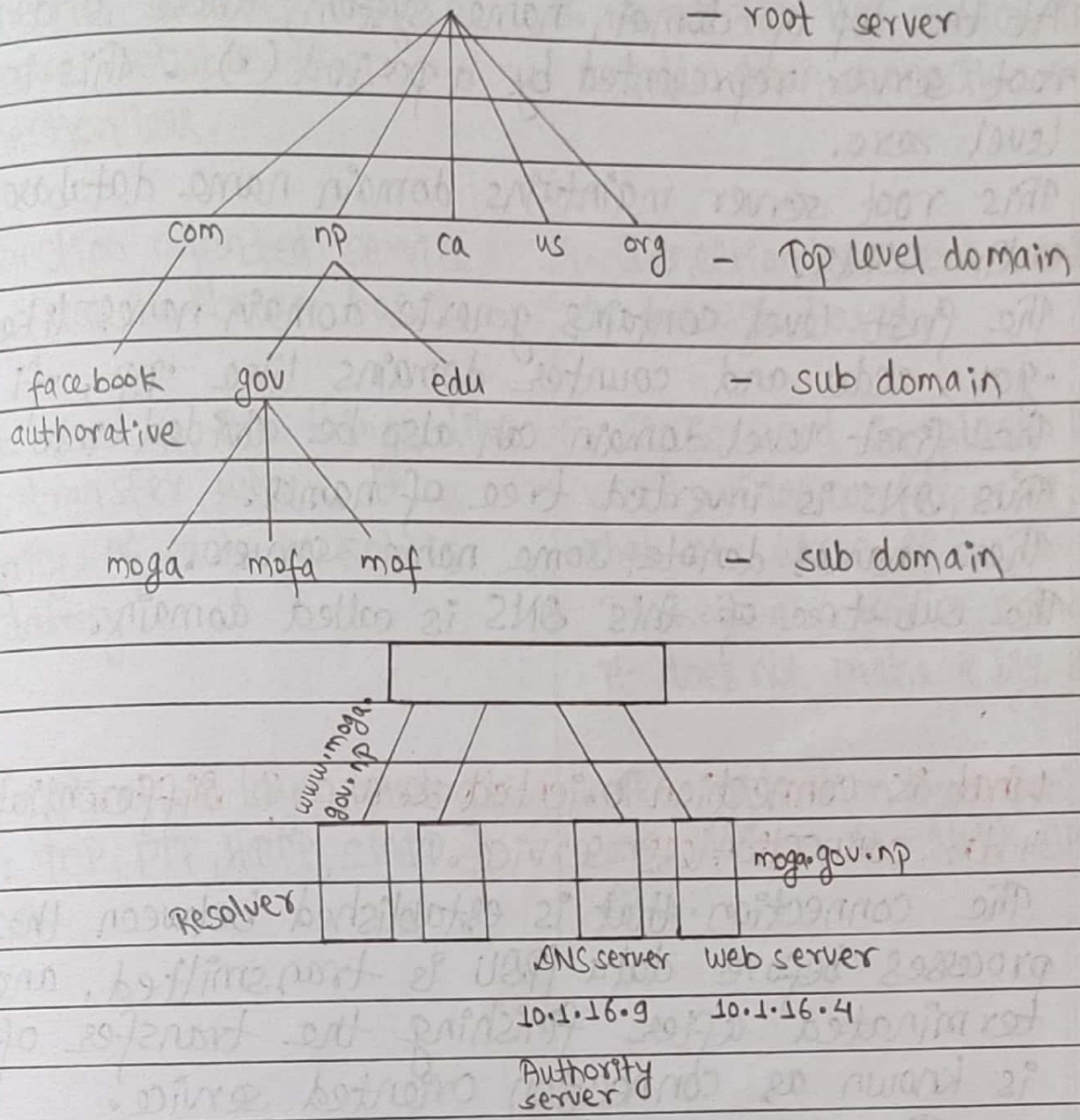


Fig :- DNS

- DNS (Domain Name System) is hierarchical sets of names used to convert domain name into IP address.
- Each name at certain level represents domain.
- Each domain consists of different name servers and other client computers.
- DNS can be maintained in flat structure but also it is not

efficient for large networks.
- At the top of domain name system, there is a null root server represented by a period (.). This is called level zero.
- This root server maintains domain name database of entire DNS.
- The first level contains generic domain names like .com, .gov, .edu and counter domains like .np, .fi, .us, .in,
- The first level domain can also be divided into sub-domains.
Thus, DNS is inverted tree of names.
- These names denote some name server.
- The sub-tree of this DNS is called domain.

What is connection oriented service? Differentiate it with connectionless service.

→ The connection that is established between the peer processes before data PDU is transmitted, and then terminated after finishing the transfer of data is known as connection oriented service.

The differences between connection oriented service and connectionless services are:-

Connection oriented	Connection less
1. Authentication is needed.	1. Authentication is not needed.
2. Connection oriented protocol makes a connection and checks whether message is received or not and sends again, if an error occurs.	2. Connectionless protocol does not guarantees a delivery.

	Connection oriented	Connection less
3.	Connection oriented service is more reliable than connection less.	3. Connection less service is less reliable than connection oriented.
4.	Connection oriented service interface is stream based.	4. Connection less service interface is message based.
5.	It is used in the things like file transfer, where the integrity of each packet is mandatory.	5. It is used in places like VOIP, video conferencing, voice chat, etc where if one or two packets are lost or out of order, it does not make a big difference.
6.	The application layer protocols are: TCP, FTP, HTTP, SMTP & Telnet.	6. The application layer protocols are UDP, TFTP, SNMP, DHCP & DNS.

What is subnetting? Assume a class C network and divide it into four subnets. What is the value of new subnet mask?

→ Subnetting is the process of breaking down a network into sub-networks.

- It is required to make efficient use of IP address, and reduces the wastage of IP address.

Numerical:

Assume an IP address as: 192.22.22.0/24.
For four subnets we need ($2^2 \geq 4$) 4 bits to borrow from host portion.

192.22.22.	00	000000	/24
192.22.22	00	000000	26 ⇒ 192.22.22.0 /26
192.22.22	01	000000	26 ⇒ 192.22.22.64 /26
192.22.22	10	000000	26 ⇒ 192.22.22.128 /26
192.22.22	11	000000	26 ⇒ 192.22.22.192 /26

∴ New subnet mask = /26

= 11111111.11111111.11111111.11000000/26

= 255.255.255.192 /26.

classmate
Date
Page

Discuss multimedia networking application.

→ Multimedia network application is any network application that employs audio or video.

- Multimedia technology enables humans to use computers capable of processing textual data, audio and video, still pictures and animations.
- In the recent years, there has been an explosive growth of new applications on the internet as discussed above, referred as continuous media applications and require services different from traditional elastic applications like email, web, remote login, etc. They also differ from download and then play applications. Especially the new applications requires high quality communication latency. One key issue for supporting new multimedia networking applications is how to get the high quality for communication latency, and internet is the one which provides no latency guarantee. Another key issue is how to improve the internet architecture to provide support for the service required by multimedia applications.

Hinderance for multimedia in today's internet causes end-to-end delay and packet jitter. So, to overcome this, some fundamental changes to the internet should be made. The Internet service Provider (ISP) should upgrade their network well to meet the demands. Another approach to make small changes at the network and transport layers are required.

Write short notes on:

a) HTTP :-

HTTP works with the world wide web, which is the fastest growing and most used part of the Internet. One of the main reasons for extra ordinary growth of the web is the ease with which it allow access to information. A web browser is a client-server application, which means that it requires both a client and a server component inorder to function. A web browser presents data in multimedia formats on web pages that use text, graphics, sound, and video. The web pages are created with a format language called Hypertext Markup Language (HTML). HTML directs a web browser on a particular web page to produce the appearance of the page in a specific manner. In addition, HTML specifies locations for the placement of text, files, and objects that are to be transferred from web browser.

Hyperlinks made the world wide web easy to navigate. A hyperlink is an object, word, phrase, or picture, on a web page. When that hyperlink is clicked, it directs the browser to a new web page. The webpage contains, often hidden within its HTML description, an address location known as Uniform Resource Locator (URL).

b) Backbone :-

It is a part of computer network that interconnect various pieces of network, providing a path for the exchange of information between different LANs or subnetworks. A backbone can tie together diverse networks in the same building, in different buildings in a campus environment or over wide areas. Normally, the backbone's capacity is greater than the networks connected to it.

A large corporation that has many locations may have a backbone, network that ties all of the locations together, for example; if a server cluster needs to be accessed by different departments of a company, that are located at different geographical locations. The pieces of the network connections that bring these departments together is often mentioned backbone. N/w congestion is often taken into consideration while designing backbones.

One example of a backbone network is the Internet backbone.

Encapsulation:-

- Encapsulation is the process of changing data into suitable form so that data can be transferred through different layers and ultimately to destination.
- Usually starts from the 4th layer i.e. transport layer.
- Is the process of adding headers and trailers to the data.
- At the senders end in transport layer, the message is added with header and trailer containing source port address and destination port address. This is now called segment.
- The segment from transport layer is added with header containing source IP address and destination IP address in network layer. This is now called packet.
- The packet in the network layer are added with some header containing source MAC address and destination MAC address in the data link layer. This is now called a frame.
- Frames are converted into bits in the physical layer so that it can be transmitted through transmission-media.
- At the receiver end, these headers and trailers are removed by the respective layers to receive the original message.

* IP Addressing is the process of changing the segment from transport layer into packets by adding source IP address and destination IP address at the sender's end.
  - At the receiver end, the IP addresses are removed by the network layer.

IP Address:-

- 32-bit address given to a computer to identify its logical address.
- Single MAC address cannot specify computer in different network uniquely so, IP address was introduced.
- It is used when packets are to be forwarded in different networks.
- Has four parts separated by dot.
- Each part contain number from 0-255.

Multimedia and Applications:

- Networked applications that transmits and receives audio and video over the Internet.
- Many multimedia applications are highly sensitive to end-to-end delay and delay variations, but can tolerate occassional loss of data.

Applications:

1) Streaming stored audio/video
2) Streaming live audio/video
3) Real time interactive audio/video.

1. Streaming stored audio and video:-
- In this application, client requests on demand compressed audio or video files stored on servers.
- Stored audio files might be audio from professor's lecture, rock songs, symphonises, etc.
- Stored video files may be video lectures or movies, television shows, etc.
- Has three keys:

a) Stored media:-
- Multimedia content prerecorded and stored at the server.
- As a result, user may pause / rewind, fast-forward or index through multimedia content.
- The time from when a client makes such a request until the action is clear at the client should be order of one to ten seconds for acceptable responsiveness.

b) Streaming:-
- In streaming stored audio / video the client begins playing of the audio / video files a few second after it begins receiving the file from the server.
- This feature is known as streaming.

c) Continuous Playout:-
- Original timing of the recording.
- Places clients to lay constraints on the data delivery.

2. Streaming Live Audio and Video :-
- Similar to traditional broadcast radio and television except that transmission takes place over the internet.
- Allows user to receive a live radio or television transmission emitted from any corner of the world.
- But, it is not stored, so a client cannot fast-forward through media.
- However, with logical storage of received data other interactive operations like pausing / rewinding are possible.
- Delays of upto tens of second from when the client requests the delivery / playout of a live transmission to when playout begins, can be tolerated.

3. Real Time Interactive Audio Video :-
- Allows people to use audio/video to communicate with each other in real time.
- Real-time Interactive audio over the internet is often called Internet phones.

Multicast Routing :-

- The transport and network layer protocols we have studied so far provide for the delivery of packets from a single source to a single destination. Protocols involving just one sender and one receiver are often referred to as unicast protocols.
- A number of emerging network applications require the delivery of packets from one or more senders to a group of receivers. These applications include bulk data transfer (eg: the transfer of a software upgrade from the software developer to users needing the upgrade), streaming continuous media (e.g., the transfer of the audio, video and text of a live lecture to a set of distributed lecture participants), shared data applications (e.g., a whiteboard or teleconferencing application that is shared among many distributed participants), data feeds (e.g., stock quotes), and interactive gaming (e.g., distributed interactive virtual environments or multiplayer games such as Quake). For each of these applications, an extremely useful abstraction is the notion of a multicast: the sending of a packet from one sender to multiple receivers with a single "transmit" operation.
- In this section, we consider the network layer aspects of multicast. We continue our primary focus on the Internet here, as multicast is much more mature (although it is still undergoing significant develop and evolution) in the Internet than in ATM networks. We will see that as in the unicast case, routing algorithms again play a central role in the

network layer. We will also see, however, that unlike the unicast case, Internet multicast is not a connectionless service -- state information for a multicast connection must be established and maintained in routers that handle multicast packets sent among hosts in a so-called multicast group. This, in turn, will require a combination of signaling and routing protocols in order to set up, maintain, and tear down connection state in the routers.