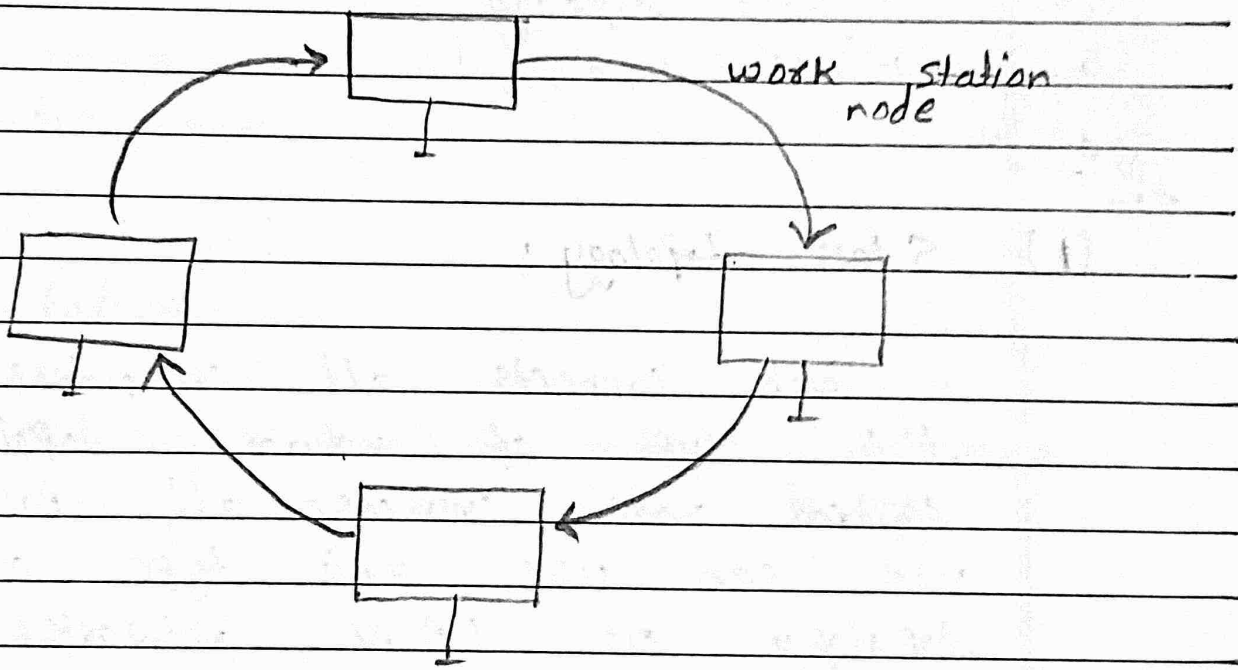
Date 14.5.24
Page

Networking

What is networking?

Connection of group of computers which is used to share their resources from one computer to another.



Topology:

Architecture design of any system in a special pattern is called topology.

The structure of the network and how each component is connected to the others are defined by the

P.T.O.

network topology: Topology comes in two flavours i.e. "Logical topology and physical topology."

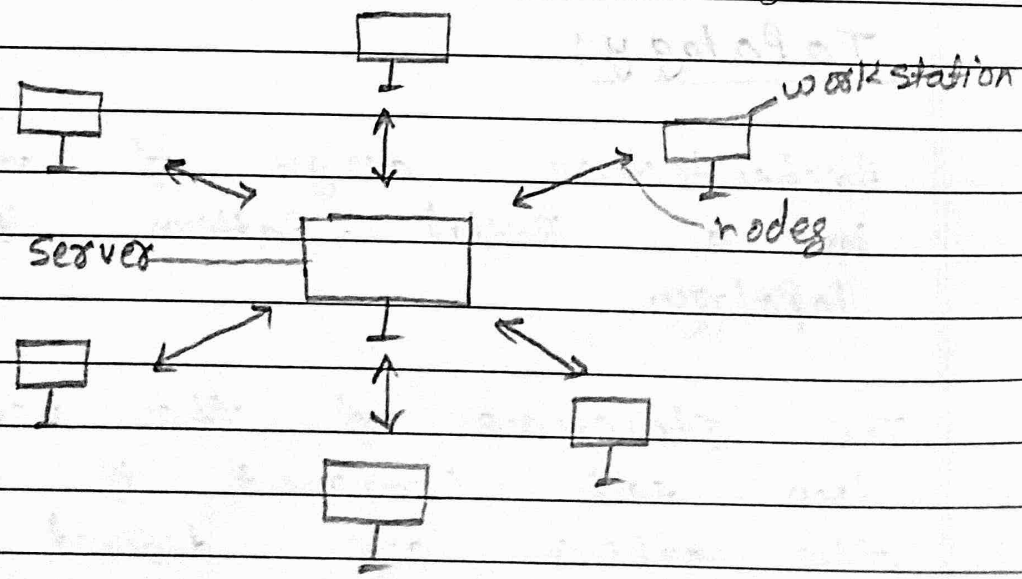
Mainly we have six types of topologies.

(i) Star topology
(ii) Bus topology
(iii) Ring topology
(iv) Tree topology
(v) Hybrid topology
(vi) Mesh topology

Date 16.05.24

(i) Star topology:

A hub connects all computers in this type of network topology. A central node connects all further nodes. We can use this type of network topology on LAN networks due to its low cost and ease of setup.



Advantages of star topology

(i) Network failure prevention:

Only the affected nodes will fail while the remaining nodes will continue to function.

(ii) Performance:

High Performance with a small number of nodes and very little network traffic.

(iii) Upgradation:

This Topology makes adding, deleting and moving devices very simply.

Disadvantages of star topology

(i) Expensive:

The cost of installing star topology is high due to the special architecture designed by the user.

P.T.O.

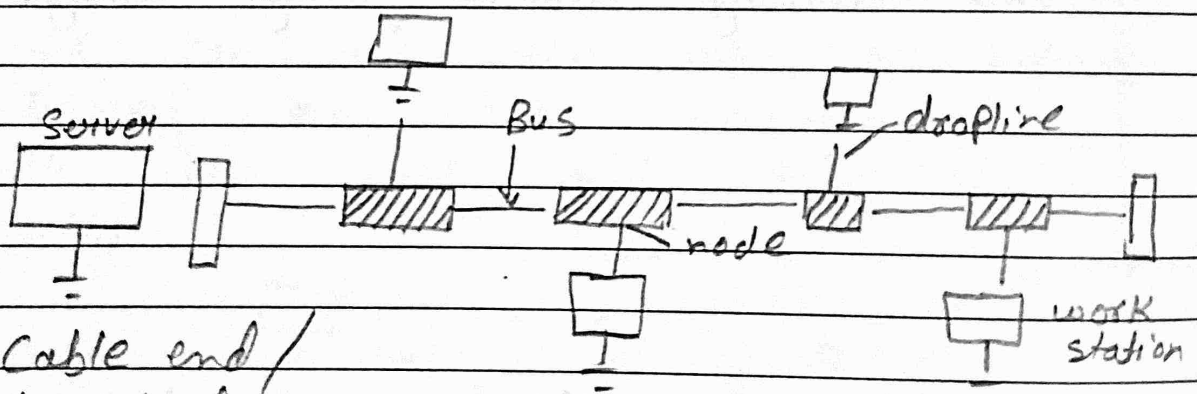
(ii) Slow connection :

Heavy network traffic can sometimes significantly slows the bus.

(02) Bus topology :

Bus topology employs a single cable (Bus) to connect all the nodes. The main cable serve as the network "spine". All nodes in a bus topology are like to the "Taps and drops" lines via the bus.

Droplines are the connection between the central wires of the bus and the nodes in the's case.



Date 17.5.24
Page

Advantage of bus topology :

(i) **Less Cabling :**

A common wires connects all nodes in a bus topology so that less cables are required to connect the computer.

(ii) **Less expensive :**

Bus topology is less expensive because it uses a common wire for transmission of data.

(iii) **Small network :**

This is best suited for situations where only a few computers are required for connection establishment.

(iv) **Upgradable :**

A new node can be added or removed in this topology without affecting the other nodes.

P.T.O.

Disadvantages

(i) Reduced signal strength:

To connect a more significant number of nodes we must increase the number of taps, droplines and the central cable and increasing these things will weaken the signal.

(ii) Core failure:

If the main central cable becomes damaged or fault the entire network will be fail.

(iii) Low security:

There ~~are~~ is a significant security issue because all nodes in the network can access what data is ~~transmitted~~ to other nodes in the network.

(03) Ring Topology:

Ring topology is a topology in which each computer is linked to other on both sides. The last computer is linked to the first two forming

a ring. This topology enable each computer to have exactly two neighbours.

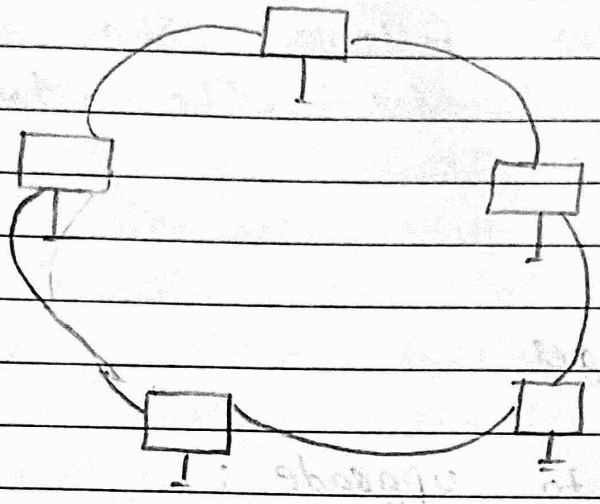


Fig of ring topology

The central computer in this topology is the monitor station which is incharge of all operations. Devices used tokens for data transmition between them.

ADVANTAGES

Token System:

Only nodes that have token can have transfer data.

Less cabling:

As every node manages the cable to its closest neighbour it requires less cabling.

P.T.O.

(iii) Trouble shooting:

It is less challenging to manage and install because the nodes and cables follows the single way to transfer the data easily discernible.

Disadvantages

(i) Difficult to upgrade:

Addition and removing nodes in problematic because it disturb the network activity.

(ii) Failure of a network:

When one system crashes it disturbs the overall network activity.

Date 20.5.24
Page

① Tree topology:

Tree topology is also known as hierachical topology as the root node connects all other nodes to form a hierarchy. This topology is also known as a star Bus topology, because it combines several star topologies into a single bus.

Tree topology is a standered network topology similar to Bus and star topology.

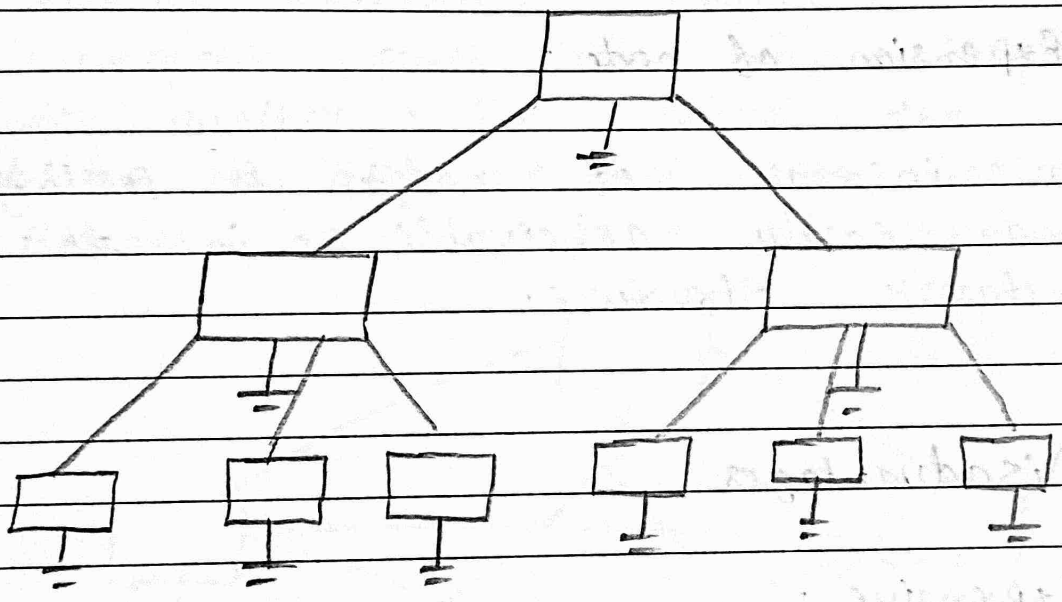


Fig of tree topology

Data flows from top to bottom in this network. It is a multipoint connection with a non-robust because the topology crashes if the backbone fails.

P.T.O.

ADVANTAGES

(i) Structuring :

It is in structuring as the tree like, shapes allows any node to hold its child.

(ii) Interconnection:

All nodes can connects to the large and intermidate networks.

(iii) Expension of node :

An increase of nodes is possibly and easily achoivable in this network structure.

Disadvantages

(i) Expensive :

Managing each node in its child may be in efficient, cabling cost will rise as well

(ii) Network failure :

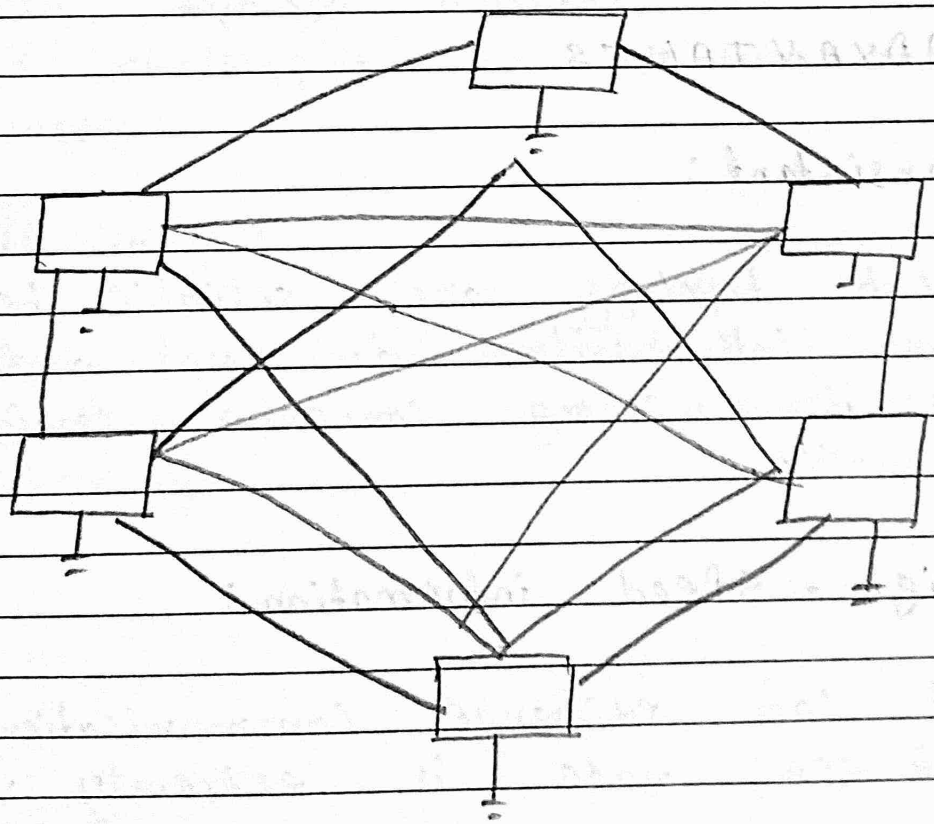
If the primary central node or other

wise fails. All other nodes may become disconnected.

Date 21.05.2024

Mesh topology:

Mesh topology is a network configuration in which you link the computers and various redundant connections. There are numerous routes from one computer to another. It lacks the switch, hub or any central computers that serves as a point of communication.



The internet is the example of Mesh topology. Mesh topology is only suitable for wireless network.

There are two types of mesh topology.

① Fully connected mesh topology
② Partially connected mesh topology

Each computer in a fully mesh topology is link to all others computers in the network and In a partial mesh topology only specific computers are connected to those with whom they frequently connected or communicated.

ADVANTAGES

① Consistant:

Mesh topology are reliable because any link failure does not disturb integration among connected computer network.

② High - speed information:

It can exchange communication between node is extremly very fast.

③ Easier recognisation:

Adding new devices could not interfair with the communication of existing devices.

Disadvantege

① Cost:

A mesh topology has more connected devices such as router and uses more transmittoas media then other topologies.

② High maintaince:

Mesh topology networks are extensive and challenging to maintain and manage.

③ Efficiency:

The number of redundent connection in this topology is high reducing network efficiency.

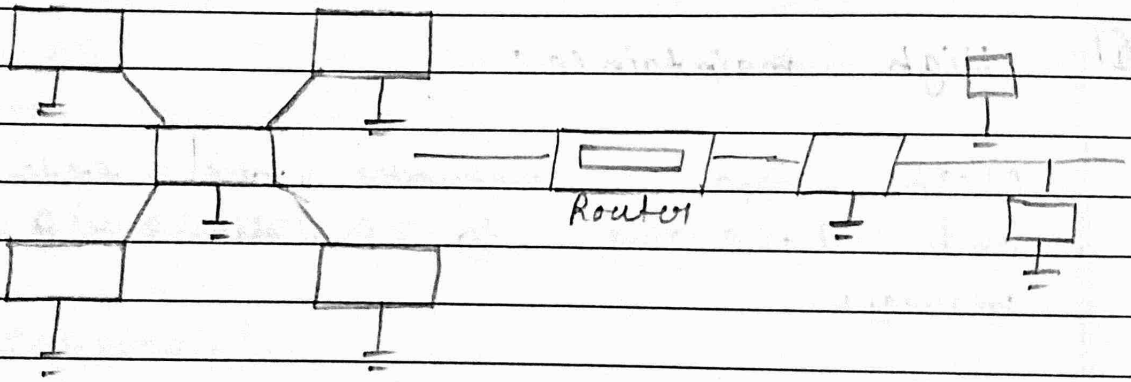
P.T.O.

22-5-24

(6) Hybird Topology :

Hybird topology is a combination of two or more of the basic topolgies, in this topology two different topologies combines to form a new topology. These topology's are used for largcd campus of the goverment institutions.

E.g. A Star-Bus topology is a hybird topology that combines the Star and bus topology.



Star topology Bus topology

Fig of hybird topology

ADVANTAGES

① Multiple advantages:

These types of network topology combined the advantages of various topologies into a single topology.

② Scalable:

Hybrid network are easily scalable as we can easily integrate the new hardware component.

③ Traffic:

These types of network topologies can handle a high traffic volume while remaining extremly Flexible and dependable.

Disadvantages:

① Expensive:

Because it combines the benifit of multiple topologies into a single topology this type of topology is quite expensive.

P.T.O.

(2) Complex Design:

Creating a hybrid topology is a difficult task because two different topologies can be adjusted in a single form.

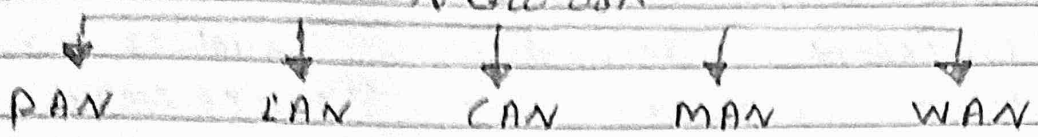
Classification of computer network

There are mainly five types of computer networks:

(1) Personal Area network (PAN)
(2) Local Area network (LAN)
(3) Wide Area network (WAN)
(4) Metropolitan Area network (MAN)
(5) Campus Area network (CAN)

Date 24.5.24
Page

Network:



(1) PAN - (

It is the smallest network of computers Bluetooth or other enforced enabled devices could be used to connect devices, it has a big low order range of connectivity, it can cover upto 30 feet in diameter. PAN network enables a single persons, Personal devices to connect with each other.

e.g. USB, Computer (PC), Phone, tablet, printer, PDA etc.

(2) LAN:

In a small network such as a building or a small office in which systems are connected. LAN network is low cost. A LAN network connects a group of computers and peripheral devices in a specific area or connected with in a limited area.

Such as: A School, Laboratory, home or office

P.T.O.

This type of computer network is a popular way to share resources. such as files, printers, games, and other application. The two important technologies involves in these networks are "ETHERNATE And WIFI". It ranges up-to 2 Km and transmittion speed is very high with easy maintaince and low cost.

(3) WAN:

A wide area network is a type of computer network that connects computer over long distances using a shared communication path, this type of computer networks can connect devices remotly. The satellite is responsible for data communication between continents and Sub-continents.

WAN can also be defined as a group of local area networks that communicate with each other with a range above 50 Kilometers.

Here we can use "LEASED-LINE" and dial up technology. It's transmittion is very low and it comes with very high maintaince and

very high cost.

· Ex. Internet

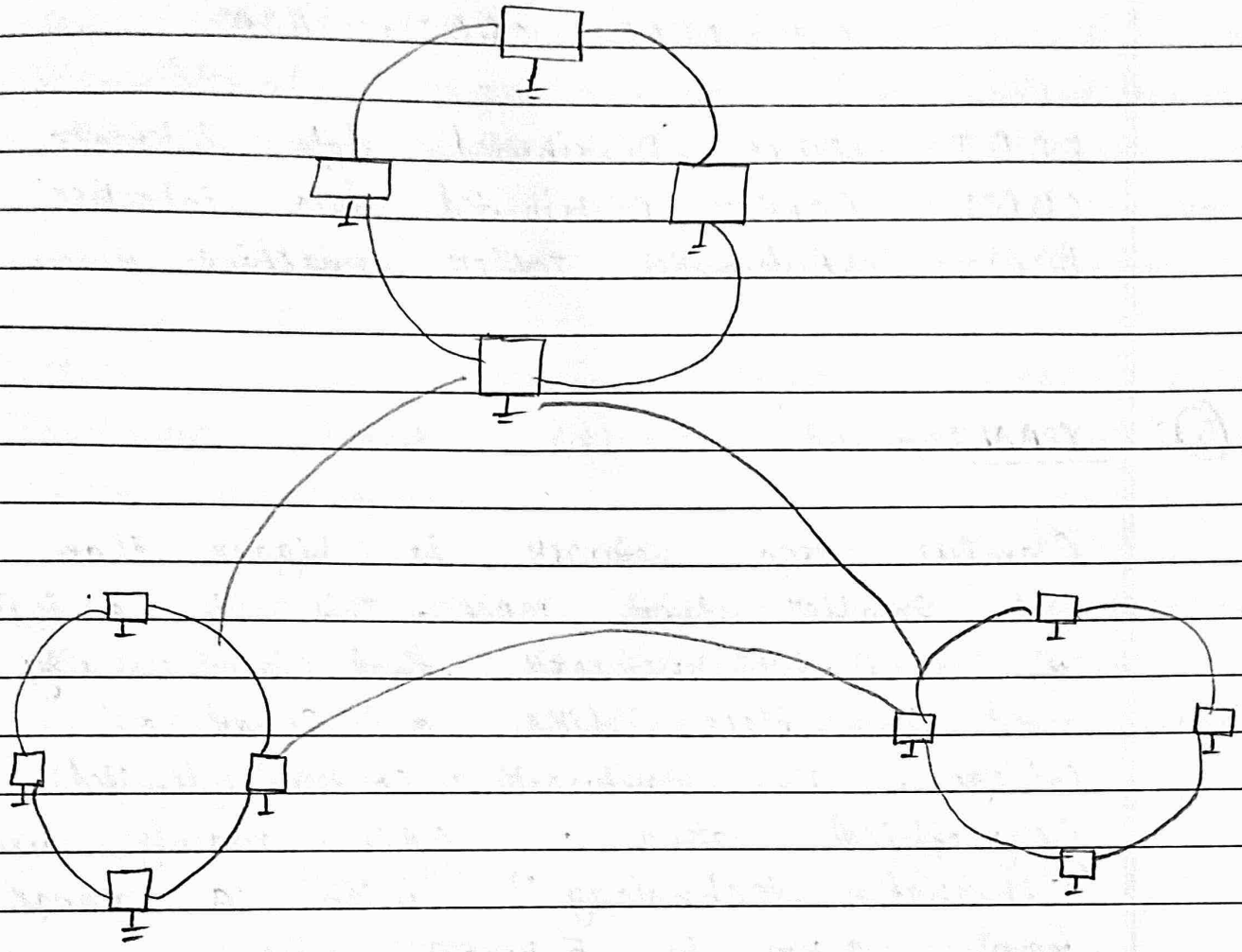


Fig of WAN

(4) MAN :-

A MAN is larger than a LAN but smaller than a WAN. This is the type of computer network that connects computer over a distance on a city, town, or metropolitan. This network mainly

P.T.O.

used "FDDI, CDDI, ATM as the technology with a range from 5 km to 50 km. Its transmition speed is average.

e.g: FDDI, CDDI, ATM

FDDI - Fibre Distributed data interface
CDDI - Copper Distributed data interface
ATM - Automatic Teller machine.

(5) CAN:

Campus Area network is bigger than LAN but smaller then MAN. This is a type of computer network that is usually used in place like a school or colleges. This network covers limited Geographical area. CAN mainly used "Ethernet technology" with a range from 1 km to 5 km.

Date 24.6.2024
Page

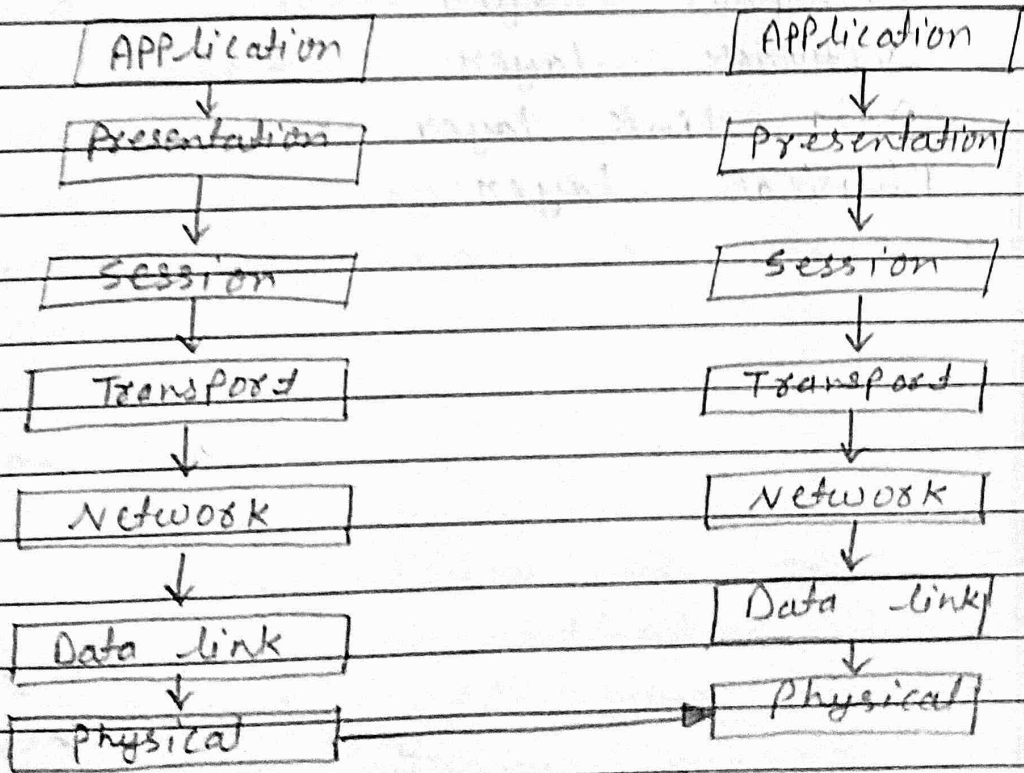
What IS OSI MODEL

OSI stands for "Open system interconnection model. It has been developed by standard organisation - ISO (" International organisation for standardization." In the year of 1984.

The two main things we have to remember is:

1. It is a seven layer architecture where each layer having specific function.

2. All the seven layers work collaboratively to transmit the data from one network to another network across the globe. (wire bridge)



P.T.O.

The OSI model created in 1984 by ISO (International organisation for Standerdization). is a reference framework that explains the process of transmiting data between computers. It is divided into seven layers that work together to carryout specialised network functions. Allowing for a more systematic approach to networking.

The OSI model consist of seven abstraction layer arranged in a drop-down order.

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

25.6.24

① Application layer :

The application layer is concern with the specific type of application itself and its standerization ed communication method for e.g. " Browser can communicate using Hypertext transfer protocol source (HTTPS) and Emails. client communicate using POP3 (Post office Protocol ver-5) and SMTP (single mail transfer Protocol).

② Presentation layer:

The presentation layer preliminary concern with the syntax of the data it self for application to send and consume. for ex. Hypertext Markup language (HTML) Javascript object Notation (JSON) and Comma seprated values (CSV) are all modeling language to describe the structure of data at presentation layer.

③ Session layer:

The session layer is responsible for network co-ordination between two seprate applications in A session. A session manages the

P.T.O.

beginning and ending of a one to one application connection and synconization conflicts. network file system (NFS) and server Message block (SMB) are commonly use protocol at the session layer.

(4) Transport layer:-

The primary focous of the transport layer is to ensure that data packets arrived in the right order, without lossing or errors or can be received clearly. if required flow control, along with error control is often a focous at the transport layer.

At this layer commonly used protocol include the transmission control protocol (TCP) a near lossless connection based protocol and the user Datagram protocol (UDP) is used to transfer the data.

(5) Network layer:

The network layer is concerned with concept such as routing forwarding and addressing across a network of nodes. the network

layer also manage flow control across the internet. The internet protocol v4 (IPV4) and (IPV6) are used as the main network layer protocol.

(6) Data-link layer:

The data link layer refers the technology used to connect two machines across a network where the physical layer already exist. It manages data-frames which are digital signals encapsulated into data packets flow control and error control of data link-layer.

The data link layer split into two sub-layers :-

(i) The media Access control (MAC) layer
(ii) Logical link control (LLC) layer

(7) Physical layer:

The physical layer refferes to the physical communication medium and technologies to transmite data across that medium at its core. data communication is the transfer of digital and electronic signal through various physical channel like Optical fibre cable and copper cabling and air medium.

P.T.O.

Date 26.6.2024
Page

The data are transfer in bid formation.

Data Communication Fundamentals and Techniques:

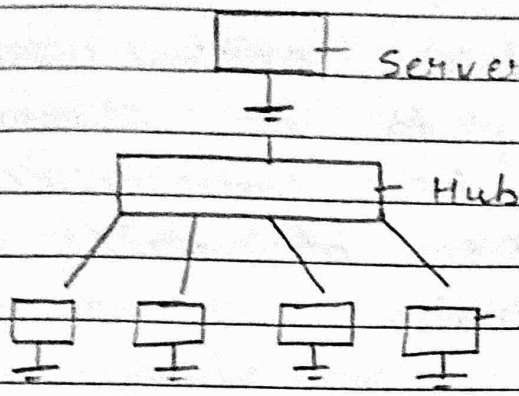
What is data communication?

Data communication is a process of sending and receiving digital data between two or more computers via transmission medium such as cable (wire or wireless).

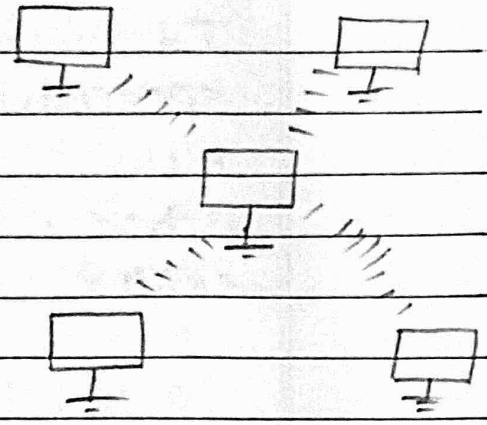
Data Communication is a process to exchange of data between two device for sending and receiving. There are main five component of data communication. They are Sender, receiver, message (data), medium and protocols.

In case of computer networks in the process of exchanging data between this device either by wireless and cable medium.

Cable medium



wireless medium



Data Communication system

It works by the three forms of systems they are as follows:

① Data Communication:

It involves a communication system which is made up of hardware and software. The message are to be transfer between the devices.

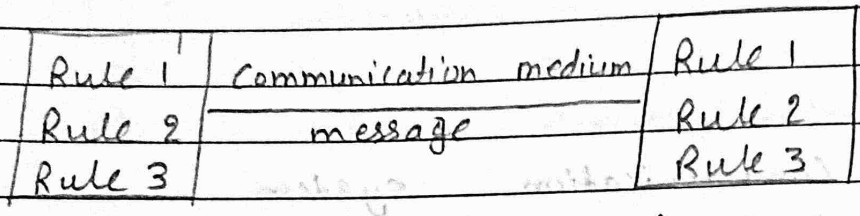
② Hardware Part:

It involves the sender and receiver devices and the intermediate devices through which the data passes.

P.T.O.

(3) Software part (Protocol) :

It involves certain rules which specify what is to be communicated, how it is to be communicated and when. This type of rules are called as a protocol.



1. Message :-

(i) Message is a data / information to be communicated by the sender to the receiver.

(ii) The message could be any form. It may be in form of a text file, an audio file, a video file etc.

(iii) The message can be of any size from 1 bit to megabyte.

(iv) Message can be either analog or digital. Signal formal depending on transmission media (wired / wireless).

2. Sender :

(i) The Sender is any device that is capable of sending the data.

(ii) The sender device can be in form of a computer, mobile, Laptop, telephone, video, camera etc.

3. Receiver :

(i) It is a device that receive message.

(ii) Receiver could receive its data with speed as that of transmission media band - width.

4. Transmission Medium :

(i) It is the path by which the message travels from Sender to receiver.

5. Protocols :

(i) It is an argument of set of rules used by the sender and receiver to communicate data.

A Protocol is a set of rules that governs data communication.

e.g. TCP / IP, UDP / IP, FTP etc.

P.T.O.

Date 01.7.24
Page

What --is Signal ?

Signals is an electronic wave that carries information through a physical medium. Here the data is converted into an electromagnetic signal either analog or digital and sent from sender to receiver.

Voltage and current are a few time-varying quantities that are used to represent data by varrying these quantities with respect to time. data can be transmitted similarly. Signal is also represent function of a frequency domain rather than the time domain.

Date 02.07.2024

Signal are divided into two categories based on their nature :-

(I) Analog Signal
(II) Digital signal

(I) Analog Signal:

Analog Signal is a form of electrical energy (voltage, current or

electromagnetic Power) for which there is a linear relation set blw electrical quantity and value that the signals represents.

Analog signals are continous in nature which varyy with respect of time. They can be Periodic or non-periodic. When the voltage time graph is floated we see a curve with continous value like waves. These signals are mave subjected to noise as they travell through the medium. These noises are result in information loss in the signal. Analog signal to digital signal by a process called "Sampling and quantization". Sound waves are converted to a sequence of samples by the process of Sampling.

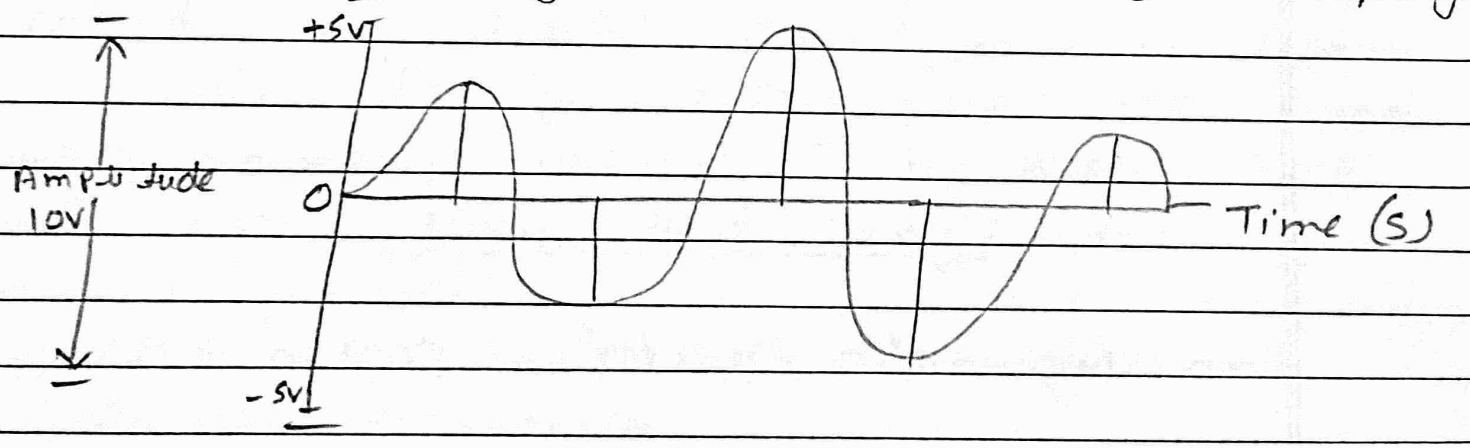


Fig of Analog signal.

P.T.O.

(2) DIGITAL SIGNALS:

This signal whose amplitude take only limited value is called a digital signal. Digital signal are discretes, They contain only distinct values. Digital signal carry binary data i.e. 0 & 1 in the from of bits. It can only contain one value at a period of time. Digital signals are represent as square waves or clock signals. Digital signals are less subjected to noise compare to Analog signal.

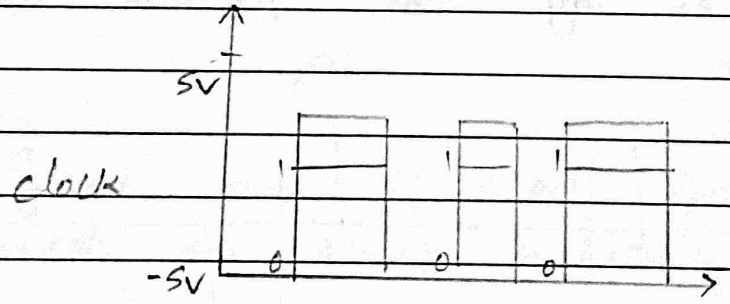
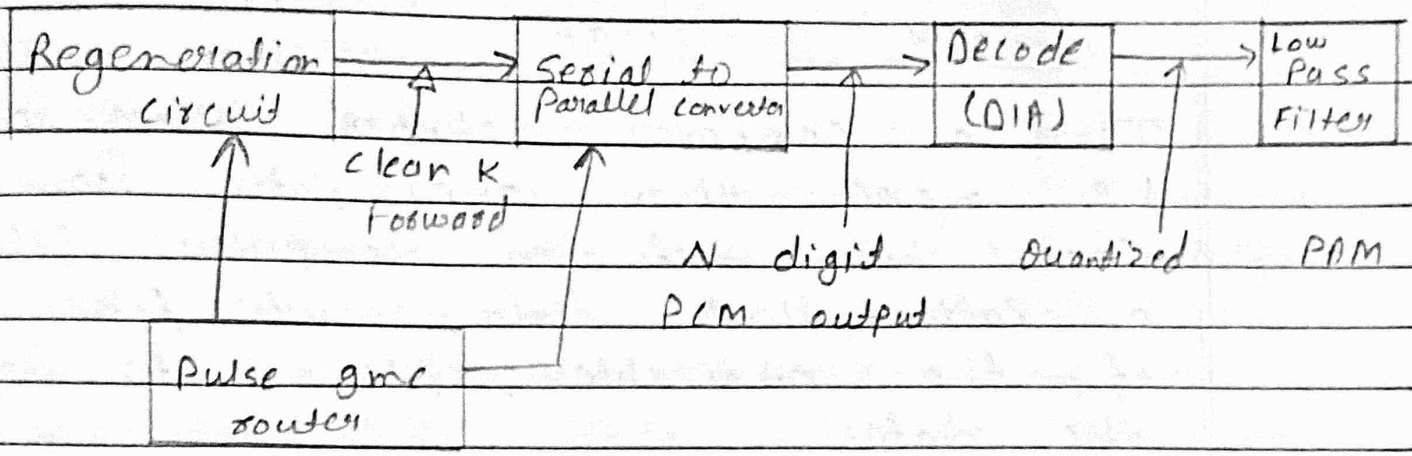


Fig of Digital signal

Date 22.07.2024

Decode (Receiver of PCM)



The message signal is the signal is being transmitted for communication and the carrier signal is a high frequency signal. Instead of a pulse train PCM produces a series of no or digits and hence this process is called as digital. This message signal is achived by representing the signal in discrete formation by the help of both time and amplitude.

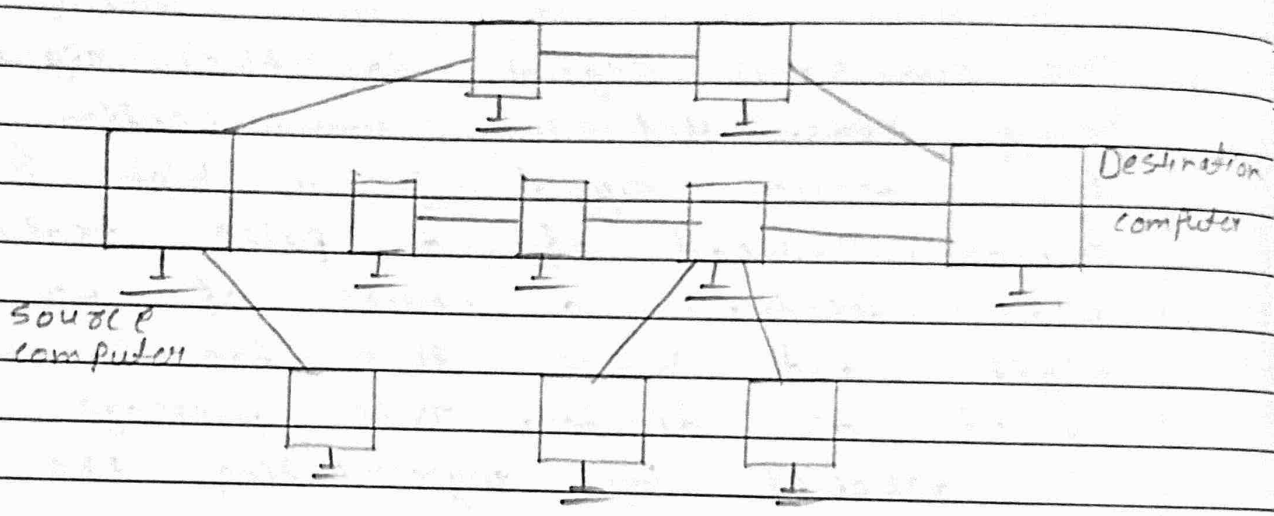
Network Switching Technique and Access mechanism

We already know that there are popular network switching techniques they are as follows:

1. Circuit Switching
2. Message Switching
3. Packet Switching

Network Switching :-

In a computer network there can be more than one path from source to destination computer. Selecting a path that data must take out of the available options to deliver the data.



We use switching techniques in computer network to connect devices and allow them to communicate with each other, switching allows multiple devices to share the same communication channel. Simultaneously As a result it improves the efficiency of the network. We use switching technique for the better performance in the network.

(1) Circuit Switching :-

We mainly used circuit switching in the traditional telephone networks. Circuit is established blw the two ends, destinated path for data to travel from one end to the other hand. Resources are reserved at intermediate switches are connected by the physical link. Once the circuit established on the dedicated path data will be transfer from one end to the other hand end as soon as the data transfer complete the circuit is disconnected.

Advantages:

(1) Well defined and Dedicated path exist for the data to travel.

(2) No waiting at any switch.

(3) Data is transmitted without any delay.

(4) Data always reaches the other end in ordered form.

Disadvantages:

(1) Channel is blocked for duration of transmission.

P.T.O.

(2) Inefficient in terms of utilization of system resources.

(3) Time required for establishing the circuit blw both end is too long, it requires more bandwidth and more expensive.

23.7.24

(2) Message Switching :-

There is no dedicated path to transfer data from sender to receiver. The message is only forwarded from hop to hop. When any intermediate switch receives the message it stores the entire message. The message is store until sufficient resources become available to transfer a to the next switch. When resources became available the forwarded message to the next switch this is called a store and forward technique.

Advantage:

(1) Channel is not blocked.
(2) More devices can share the channel.
(3) Helpful in reducing traffic conjunction as the message can be store in the route and forwarded whenever required.

Disadvantage:

① Requires enough storage at every switch to accumodate the entire message during the transmission.

accumodate = Place, living, store.

② It is extremly slow due to store and forward technique message has to wait until the subficient resources become available to transfer to the next switch.

③ Packate switching:

Entire message to be send is divided into multiple smaller size packates. This process of dividing a single message into a smaller packates is called as packatization, this small packates can one after another in a recurrance formation to the destination computer.

The packate switching is of two types:-

① Virtual circuit switching
② Datagram switching.

P.T.O.

Virtual Circuit Switching:

In virtual switching circuit the first packates informs all intermediates switches of all the packates that are following and receives the delivered packates. The first packate reserves resources into the cpu bandwidth which required for the packate as well as the system locations. All the paths and the packates then follow the same way to deliver the complete packate.

Datagram switching :-

In the datagram switching this packate is created as seprate entity and it is routed independtly through the network.

Advantage :- and Disadvantage

(1) Cost effective and easier to implemint.

(2) Use lesser bandwidth as the packates are quickly router to forward the destination.

(3) It does not take large amount of space.

(4) If Packate is lost you can request for new package/ packate.

Disadvantage:

(1) Unsuitable for application that cannot afford delay's in communication.
e.g. voice calls, conference.

(2) It also requires high installation cost.

(3) It requires complex protocols for delivering It could also leads the network problem and errors, delay in delivery or loss of packats.

Date 24.09.2024

Transport layer function and Protocol

Transport layer:

The transport layer (forth) of the open systems interconnection communication model. It is responsible for ensuring that the data packates arrive accurately and reliabely between senders and receiver. The transport layer most often uses (TCP) or user data-gram protocol (UdP). In the TCP/IP network model

P.T.O.

The transport layer comes between the application and network layer.

In the OSI model the transport layer sits blw the network layer & the session layer. The network layer is responsible for taking the data packates and sending to the correct computer. The transport layer then takes the received packates checks them for errors and sorts them. Then it sends them to the session layer of the current program running in the computer. The session layer now takes the well formated packates and uses them for the application data.

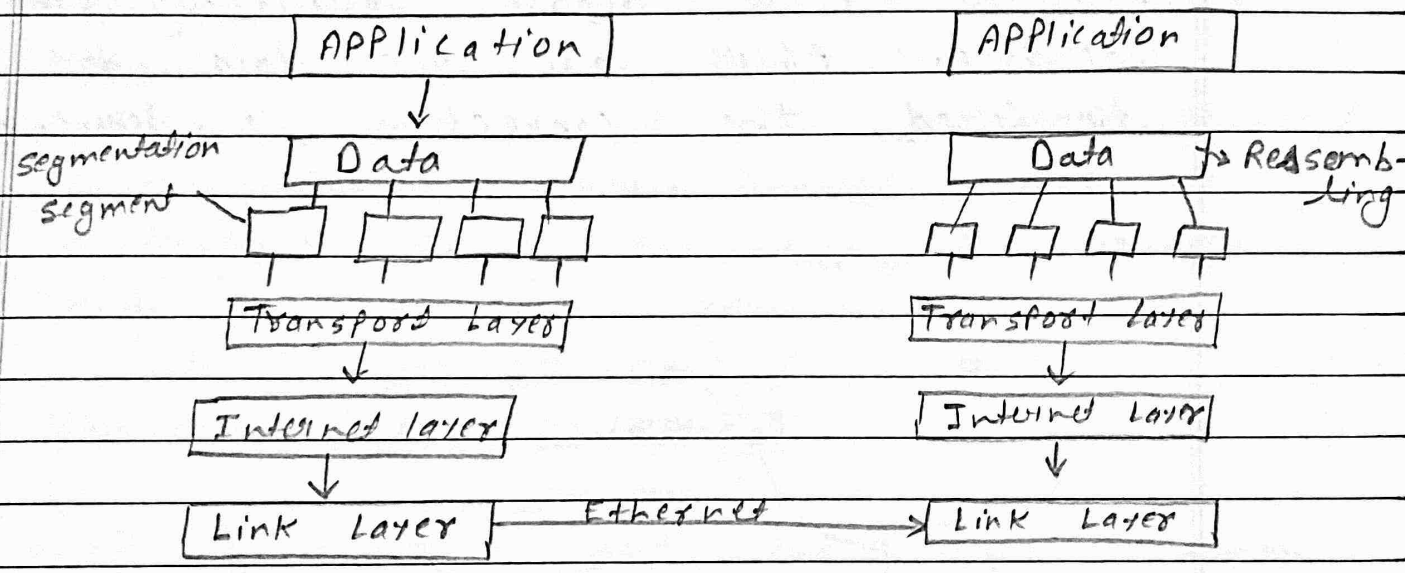
Date 29.7.2024

* Service Point addressing.

The transport layer header must include a type of address called a service point address or port address. The network layer get each packate to the correct computer. The transport layer gets the entire message to the correct process on that computer. The transport layer is responsible for process to process delivery message.

☆ Segmentation and re-assembly:

A message is delivered into transmeliable segments which each segment containing a sequence no. of This no's enables the transport layer to reassemble the message correctly upon arriving at the destination and to identify and replace packates that were lost in transmition. It give the requrration for the lost item.

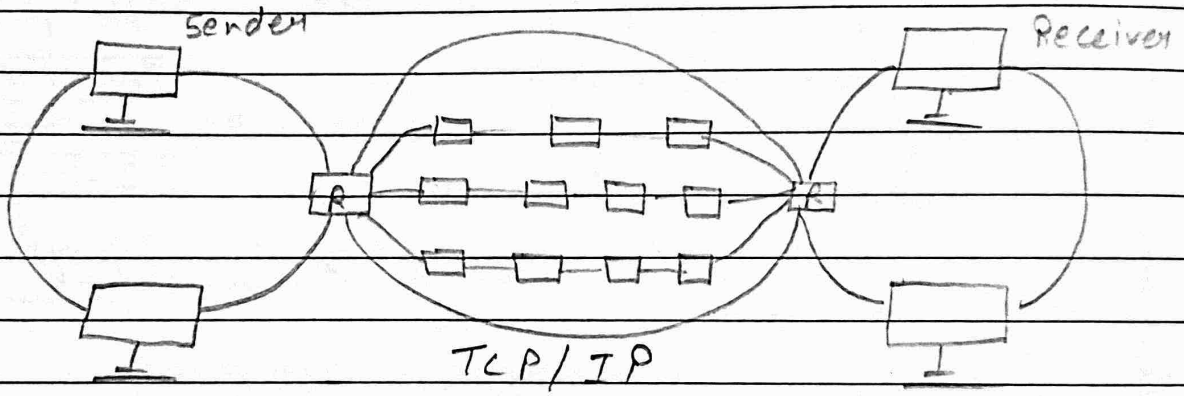


P.T.O.

Date 30-7-24
Page

Connection Control:

The transport layer can be either connection less or connection oriented. A connection less transport layer treats each segment as an independent packet and delivers it to the transport layer at the destination machine. A connection oriented transport layer makes a connection with the transport layer at the destination machine first before delivering the packates, After all the data are transfered the connection is terminated.



Flow Control:

It is also called process to process or the network to network. The performance is as same like data link layer. The transport layer is responsible to check all the overall performance for flow control at this

layer is performed end to end rather than access a single link. Data is further check the errors which is claimed by the other networks.

ERROR CONTROL:

As like the data link layer the transport layer is responsible for error control. ~~at~~ At this layer is performed process to process rather than access a single link. The sender transport layer make sure that the entire message arrives at the receiving transport layer without error (Damage, loss or duplication). Error connection is usually acheived through retransmission.

Transport Layer protocol:

UDP and TCP are the most common transport layer protocol.

(i) UDP (User Datagram Protocol)

It stands for user datagram protocol. It is a single simple and fast transport protocol. It is for connection less transmission. It is considered uncredible because it does not use acknowledgements and retransmissions, so packets may be lost.

P.T.O.

UDP is best for real time data where speed of delivery is more important than reliability such as for video conferencing uses.

(ii) TCP (Transmission Control Protocol) :-

It stands for Transmission Control protocol. It is the more feature-rich transport protocol. It is connection oriented. It uses synchronization and acknowledgements messages to ensure delivery. It retransmits and re-orders packets if needed. It can negotiate sending and receiving rates. TCP is slower the UDP. TCP is the most common protocol on the network.

Date 31.7.2024

Multiple Access protocol and networking

Multiple access protocol are set of multiple protocols operating in the medium access control sublayer (MAC) sublayer of the open system Interconnection (OSI) Model. These protocols allows a number of nodes or users to access a shared

networks channel several data streams originating from several nodes are transfered through the multipoint transmission channel.

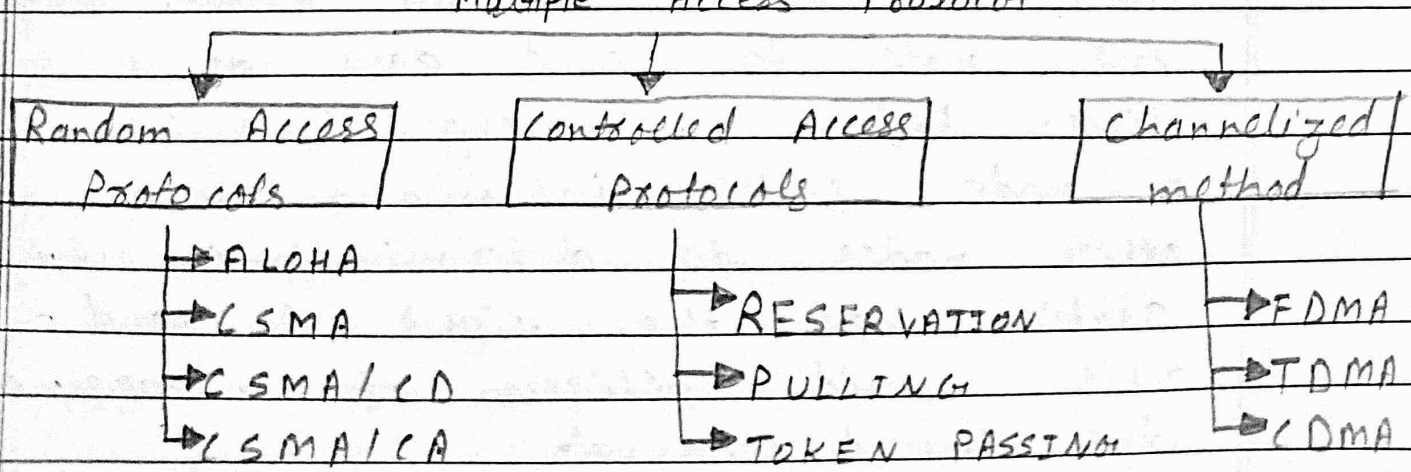
The objectives of multiple access protocols are optimization of transmission time, minimization of collissions and avoidance of cross talks.

Categories of multiple Access Protocols

Random Access Protocol | control Access Protocol | channelized Method

Multiple Access protocol can be classified into three categories they are Random access protocol, controlled access and channalized method.

The structure can be shown like this:



Date 05-8-24
Page

① Random Access Protocol :

Random Access Protocol assign priority to all connected nodes. Any nodes can send data if the transmission channel is Idle, No fixed time of or fixed sequence is given for data transmission.

The four accessing nodes are used for data transmission, they are as follows:

① ALOHA - Advocates of Linux open source Hawai Association.
② CSMA - Carries sense multiple access
③ CSMA/CD - Carries sense multiple access with collision detection
④ CSMA / CA - Carries sense multiple access with collission avoidance

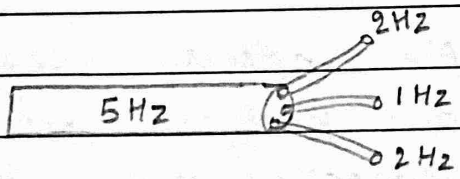
② Controlled Access Protocol :-

Controlled access Protocols allows only one node to send data at a given time. before initialing transmission a node seeks information from other nodes to determinatione which station has the right to send. This avoid collission of message on the shared channel.

The station can be assigned the right to send by the following channels they are reservation, polling, token passing.

③ Chanellization method :

Chanellization method a set of methods by which the available bandwidth is divided along the different nodes for simultaneous data transfer.



There are three channels which are used for data transfer

① FDMA - Frequency division multiple access.
② TDMA - Time division multiple access.
③ CDMA - Code division multiple access.

Date - 07. 08. 2024

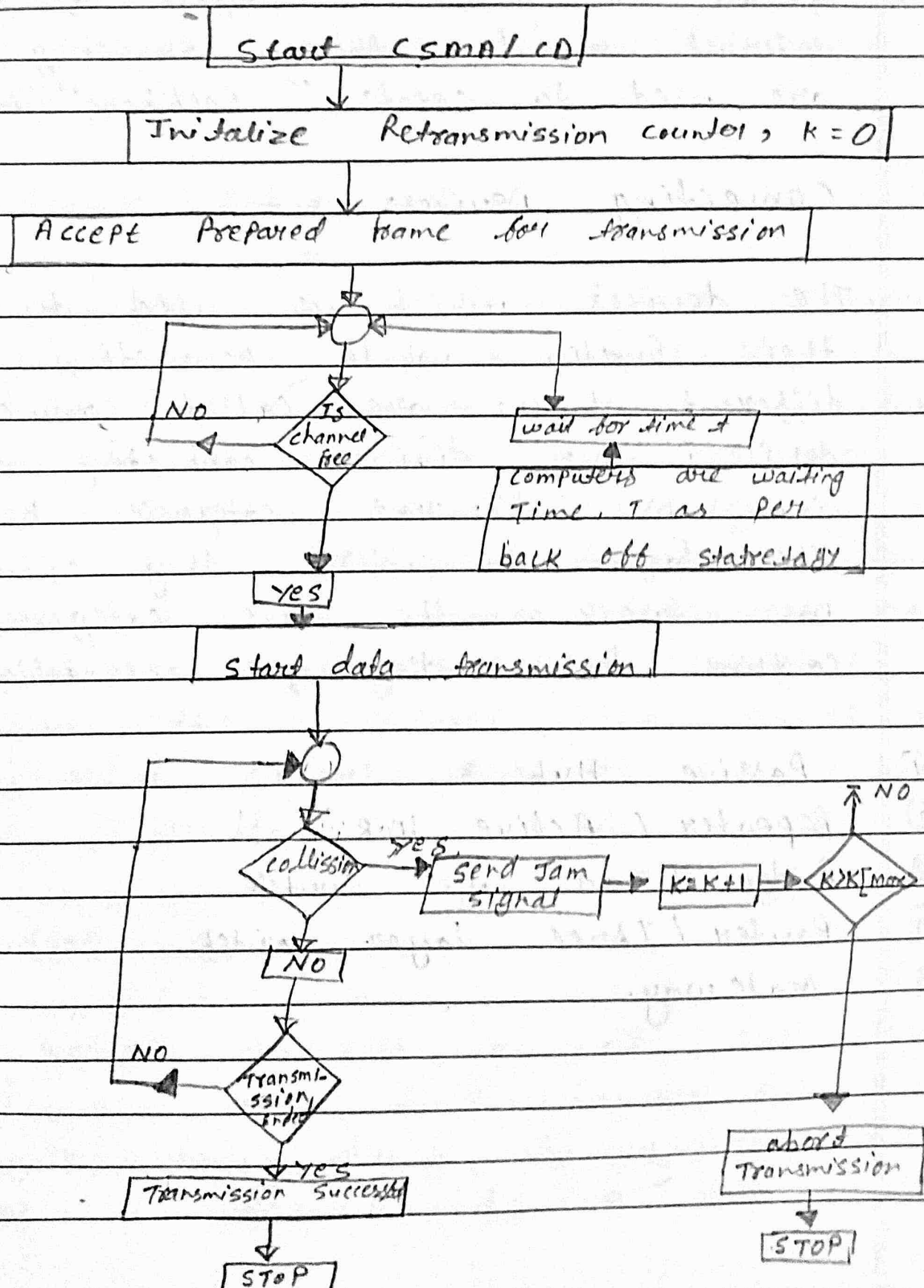
CSMA / CD :-

The network protocol for carrier transmission known as CSMA/CD runs at the medium access control (MAC) player. The shared channel for communication is detected or heard and transmission are postpond until the channel is clear by detection transmission from other stations the collision detection technique finds collisions:

Carrier senses multiple access with collission detection is a protocol used by computer "Ethernet" networks. It stops computers from sending information on the same ethernet wire at the same time with this rule a computer will check that the wire is not being used before it sends information this ability to check is called "carrier senses", This rule is used when many computers can use the same connection. This is called "multiple access". If computers do send information at exactly the same time, the computers can tell a mistake has been made and stop sending. This is called "collission detection". When this collission

occurs the computers stop sending info. wait for a information, wait for a random amount of time and then check before resending the information.

Date 12.08.2024



Date 14.8.2024
Page

ETHERNET LAN :

LANS do not normally operate in isolation they are connected to one another or to the internet. To connect lans or segment of lans we have use connecting devices. Connecting device can operate in different layers of the internet model, these connecting devices are used to create "Backbone" networks.

Connecting Devices:

The devices which is used to operate their function while connecting with different layers are called connecting devices. we divide connecting devices into five different categories based on the layer in which they operate in network, the five categories contains devices they are as follows:

1. Passive Hub
2. Repeater / Active Hub
3. Bridge / Two layer switch
4. Router / Three layer switch
5. Gateway.

① Passive HUB:

A Passive hub is just a connector, it connects the wires coming from different branches. In a star topology Ethernet LAN, a Passive hub is just a point where the signal coming from different station collide it locate below the physical layer in the internet model.

② Repeater / Active HUB:

A repeater is a device that operates only in the physical layer. Signals that carry information within a network can travel a fixed distance before attenuation indanges the integrity of the data. A repeater receives a signal and before it becomes too weak or corrupted, regenerates the original bit pattern the repeater then sends the refreshed signal. Repeater can extend the physical length of a LAN.

③ Bridges:

A bridge operates in both the physical and the data link layers. As a Physical layer device it regenerate the signal it receives. As a data link.

P.T.O.

layer1 device the bridge can check the device physical (MAC) address, sources and destination contained in the frame. A bridge has filtering capacities. It can check the destination address of a frame and decide if the frame should be forwaded or drop. A bridge has a table that maps addresses to codes. A bridge doesn't change like the physical address contained in the frame.

Type of bridge:

① Transparent Bridge:

A transparent bridge is a bridge in which the stations are completly unaware of the bridges existance. If a bridge is added or deleted from the system reconfigration of the station is unnecessary According to the "IEE 8021" specification a system equipped with transparent bridge must meet three criteria.

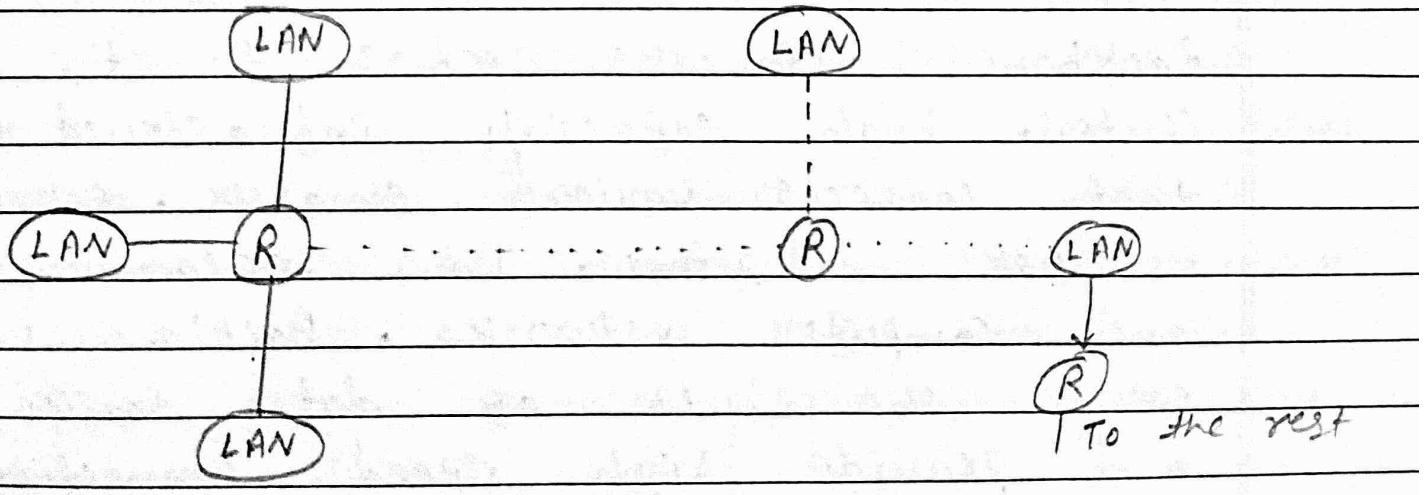
① Frames must be forwarded from one station to another.

② The forwarding table automatically made by "learning frame" movements networks.

③ Loops in the system must be prevented.

④ Routers:

A Three layer switch is a three layer device that routes packets based on their logical address (through IP) (Host to Host addressing). Routers is faster and more sophisticated. The switching fabric in a router allows faster table look up and ~~sophisticated~~ and forwarding. A router normally contains LANS and WANS in the internet and has a routing table that is used for making decisions about the route. The routing table are normally dynamic and are updated using d routing protocols.



P.T.O.

Date 03-9-2021
Page

(5) Gateway :

A Gateway is normally a computer that operates in all five layers of the internet or seven layer of OSI model. A gateway takes an application message, reads it and interprets it. This means that it can be used as a connecting device between two internetworks that used different models. The Gateway connecting the two systems can take a frame as it arrives from the first system, move it up to provide security. The Gateway is also used to filter unwanted application layer messages.

Backbone Network :

Backbone networks refers to the central high capacity infrastructure that connects various smaller, peripheral networks together. In telecommunication and computer networks. Backbone network carry the bulk of data traffic and provide high speed connection between different systems, locations and networks. such as LAN, MAN and WAN.

Backbone networks typically

consist of high performance routers, switches and fibre optic links designed to handle large volume of data over long distances they are critical foundation of the internet, corporate networks and large scale service provider.

Date - 04.09.2024

Network layer function and Protocols

Function of the network layer:

The main function of the network layer or layer 3 of OSI model is delivery of data packats from the source to the destination across multiple "hops or links". It also control the operation of the subnet.

When data is to be sent the network layer accepts data from the transport layer and sends to the data link layer. The reverse procedure is done during receiving data.

P.T.O.

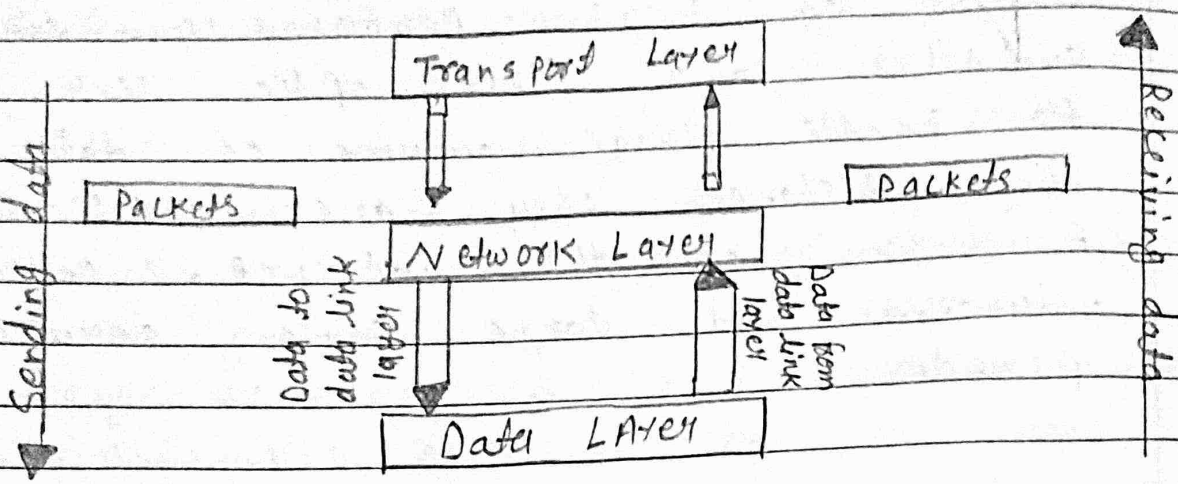


Fig Network layer function.

The network layer is responsible for routing packets from the source Host to the destination Host. The routes can be based upon static tables that are rarely changed or they can be automatically updated depending upon network conditions. This layer also provides mechanisms for conjunction control, Institution when too many packates overloaded the subnet. The network layer tackles issue like transmission delay's, Transmission time, avoidance of call dropping etc.

Date 19.9.24
Page

Overview of application layer protocols:

Overview of DNS Protocol:

An application layer protocol defines how the application processes running on diff system, passes the message to each other.

Process of DNS:

(1) DNS stands for Domain name system.

(2) DNS is a directory service that provides a mapping between the name of a host on the network and its numerical address.

(3) DNS is required for the functioning of the internet.

(4) Each node in a tree has a domain name and a full domain name is a sequence of symbols specification / specified by dots.

(5) DNS is a service that translates the domain name into IP addresses. This allows the new users of networks for utilize user-friendly name. when

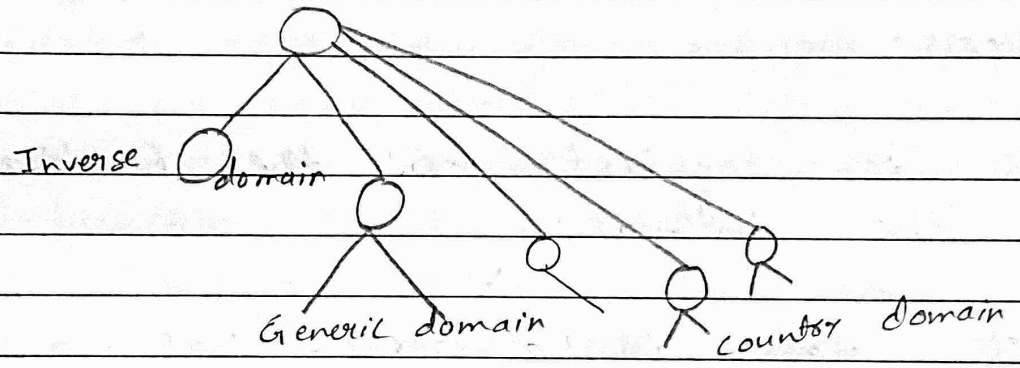
P.T.O

looking for other hosts instead of rename or remembering the IP addresses.

TCP/IP working with DNS and types

DNS is a TCP/IP protocol used on different platforms. The domain name space is divided into three different section:

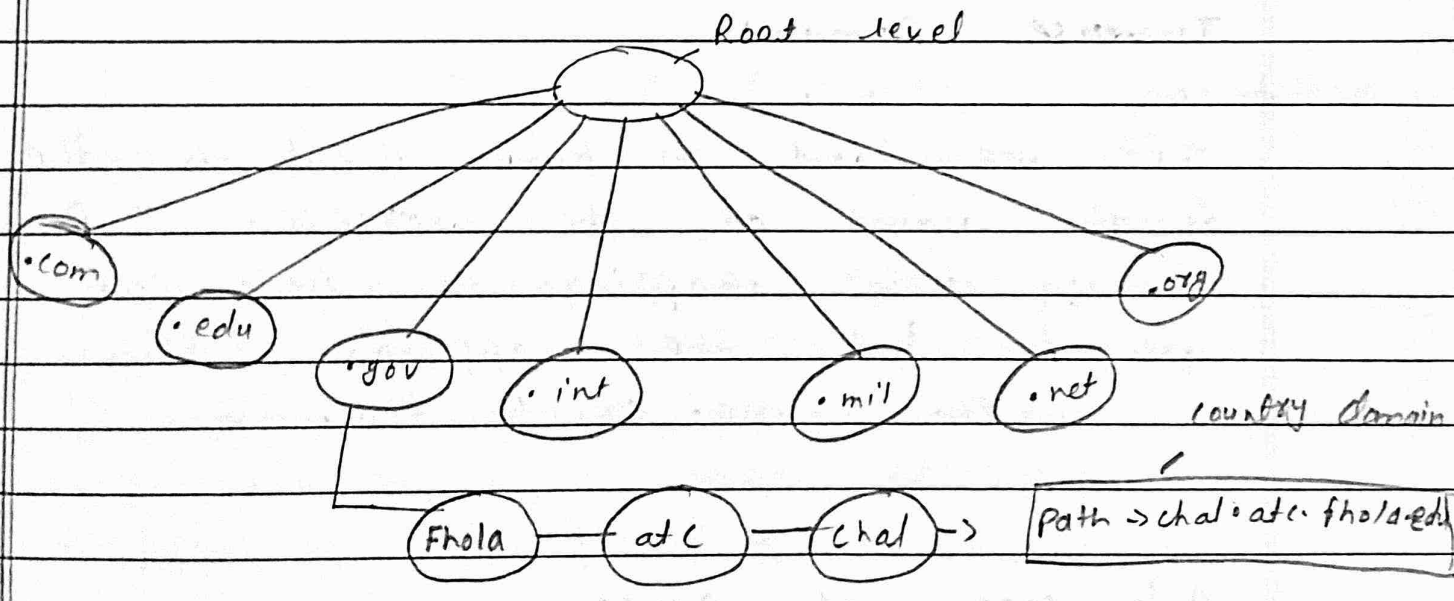
1. Generic domain
2. Country domain
3. Inverse domain.



- It defines the registered hosts according to their generic behaviour.
- Each node in a tree defines the domain name which is an index to the DNS database.

- It uses three character labels and these labels describe the organisation types.

Level	Description.
• aero	airlines and aerospace companies
• biz	Business or firms
• com	commercial organisation
• coop	cooprative business
• edu	educational institutions
• info	information service providers
• int	International organisation
• mil	Military groups
• net	Network support centers
• org	Non-profit organization
• pro	Professional individual organisation.



Date 20.9.24
Page

TYPES OF DOMAIN

There are various kinds of Domain:-

Generic Domain :-

It includes the domain which are as follows: .com (commercial), .edu (educational), .mil (military), .org (non-profit organisation) etc. are generic domain.

Country Domain :-

They are used to recognized the country site .in (india), .us (America), .uk (United kingdom).

Inverse Domain :-

If we want to know what is the domain name of the website. IP to domain name mapping. So DNS can provide both the mapping.

ex. www.crickindia.in.

Advantage of DNS:-

ADVANTAGES OF D.N.S

- The users receives important message with zero downtime.
- Through anycast technology in as instance of maintainance or downtime, the supplications are answered by the nearest node.
- DNS immediately rectifies the errors.

Disadvantages of DNS:-

- DNS is the fact that its registry can only be controlled ICANN, a non-profit organisation with roots tied in one country.
- DNS usually don't carry information about clients who initiated it.
- DNS based on the principle of master-slave relationship. It means if master server is broken or manipulated, it will be hard to access the web page or database.

Date 23.9.24
Page

Overview of WWW & HTTP

The world wide web (www) is a network of servers that use the hypertext transfers protocols (HTTP) to allow users to access online resources and website. HTTP is a protocol that allows data to be transfered between devices on the internet.

How HTTP Works:

HTTP is a client server which means that a request is initiated by the client usually a web browser and the server responds with a message.

How HTTP Has evolved:

HTTP was developed by Tim-burner's-Lee and his team between 1981 to 1991. It has evolved over time to support a wider ranges of users. such as fetching images and videos and posting content to server.

There are multiple versions of HTTP, including HTTP/1.2 and, HTTP/2 was published

in 2015 and is supported by over 98% of web browsers, HTTP/3 was published in 2022 and is supported by 99% of web browsers.

A secure variant of HTTP and HTTPS is used by more than 85% of website now a days.

Date
2.39.24

HTTP:

The hyper text transfer protocol is the foundation of the world wide web and is used to load web-pages using hypertext links. HTTP is an application layer protocol designed to transfer information between network devices and runs on top of other layers of the network protocol stack. A typical flow over HTTP involves a client machine making a request to a server which then sends a response message.

Key features of HTTP includes:

(1) Encryption: Data is encrypted to prevent unauthorized parties from

P.T.O.

reading it during transmission.

② Data Integrating:

HTTP ensure that data cannot be modified or corrupted during transfer without being detected.

③ Authentication:

HTTPS verifies that that website you are connecting to is actually the intended site and not an imposter.

Websites using HTTPS are often indicated by a lock, icon in the browser's address bar and the url starting with HTTPS //.