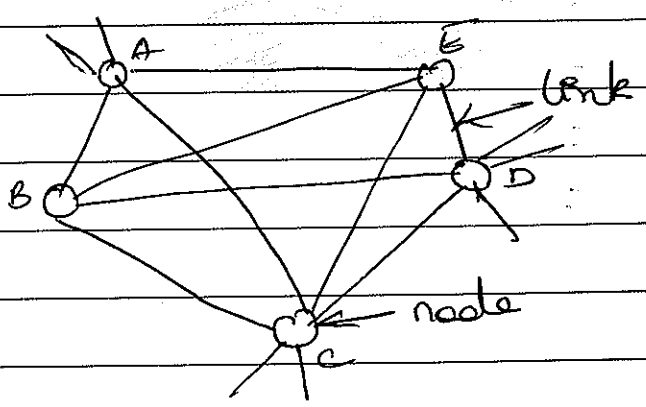
Chapter-1

Basic of Computer Network

Computer network means an interconnected collection of autonomous computers. 2 computers are said to be interconnected if they are able to exchange information.

A network is an interconnection of many nodes through which a desired entity flows or travels



Node: In communication network a node is a point where more than 2 branches meet. It is not necessary that each of them to be connected to all others. Node function is to connect the output path with an incoming path.
Eg: switch

Branch: The branch of communication network is basically a transmission medium which is either a wire or a radio channel.
Eg: copper wires, multi-pair cable, co-axial, optical cable. In communication network all the links need not be of same type.

Network: A communication network can be defined as collection of switches or nodes interconnected by transmission media (branches) carrying information bearing signals (entity) in electrical or optical form

Depending on application network is designed and deployed there are different types of network.

Telephone network: Telephone network usually called Public Switched Telephone network (PSTN) has been one of the most popular types. This network employs circuit switches as node & branches consists of transmission media. The subscriber can send/receive either analog or digital voice to/from the telephone exchange. In telephone n/w 1st a source destination path is established using signals & then only voice communication takes place.

Computer/data network: Data/computer n/w carries digital data from source to destn. Here nodes are packet switches & use store & forward mechanism. A packet switch receives information in form of packets, stores them & forwards the packet to free outgoing link. The packet switches are called routers & they transmit packets onward identifying the address of the packet. The branches are similar to the ones in telephone n/w for eg: coaxial cable, copper wire.

Computer network: 1) is a digital network
2) full duplex
3) has to have switches with storage capability

Entertainment/Distribution/Broadcast network

Earlier the broadcast network was supporting only the audio signal but today we have TV broadcast networks. It is a receive only network where user normally can't transmit. Broadcasting can be wireless for radio & terrestrial, or satellites in TV networks.

Unified/Integrated Network: Advances in computer & digital communication fields resulted in Integrated digital Networks & later Integrated Services Digital Network (ISDN). ISDN supports voice, data & also scan video from the same vendor.

Mobile Communication Network: The ability of the user to communicate even when they are on move is called Cellular Mobile Telephone Network. Initially it was designed for telephone communication, but now it provides data as well. A given area is subdivided into small cells with fixed base station which in turn is connected to a switching centre. Switching centre connects the mobile user with rest of the telecommunication

Advantages of computer network

1) Resource sharing: The goal is to make all programs, equipment & data available to anyone on the network

2) High reliability: All files can be replicated in 2 or 3 machines so if one is unavailable other copies could be used

Different Categories of Computer Network

Local Area Networks: These are privately owned networks within a single building or campus of upto few kilometers in size. They are widely used to connect personal computers & to share resources & exchange information

Metropolitan Area Network: It is basically a bigger version of a LAN. It covers a group of nearby corporate offices or a city. MAN can support both data & voice. A key aspect of a MAN is that there is a broadcast medium to which all the computers are attached.

Wide Area Network:

It spans a large geographical area usually a country or continent. If WAN has to be set up than first LAN has to be set up at different countries & the LANs interconnected to form WAN.

Chapter-2
Communication switching

Switching: A switch is a hardware or a software device that allows a connection to be established between 2 or more devices which are linked to it.

Circuit Switching: It is a direct physical connection path established between 2 computers. When a computer wants to communicate with another computer a dedicated connection is established between them over the switch. The computers then communicate using that ~~communication~~ connection. No other computer can use this portion of the connection. Circuit switching was mainly designed for telephone communication. Circuit switching is not as useful when it comes to computer communication as most of the time the dedicated line is not utilized. Even when other routes are free which are faster then one cannot change over.

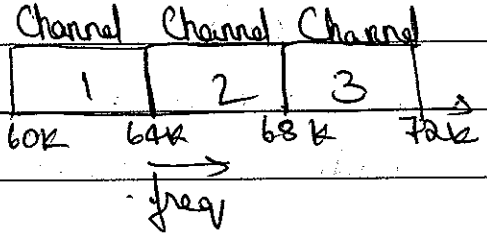
Packet switching: In packet switching data are transmitted as discrete blocks called packets which are of variable length. Each packet contains data to be transferred & also the info such as senders address & destn address

Message Switching: Message switching is better known as store & forward approach for an entire message. Computer receives a message stores it on its disk until the appropriate

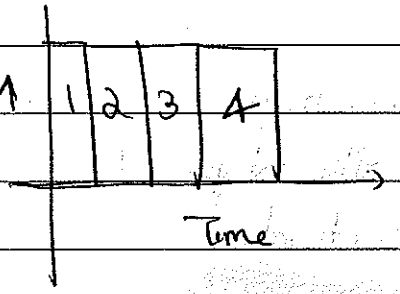
route is free & sends it along that route. Message switching specifies that the message to be forwarded should be held by the computer on its disk before it can be forwarded.

Multiplexing: It is a technique where a single channel carries more than 2 users.

Frequency Division Multiplexing: In FDM the frequency spectrum is divided among the logical channels with each user having exclusive possession of some frequency band.
eg FM



Time Division Multiplexing:
In TDM the users take turns each one periodically getting the entire bandwidth for a little amount of time.



Statistical Time Division Multiplexing
This technique monitors which machine or terminal is sending the data more frequently & in more quantity & allocates the time slices more often to those nodes. Relative inactive computers get the time slice less often while completely idle computers may not get any time slice at all.

Packet switching is of 2 types

1) Connectionless packet switching:

In this there is no pre-decided path decided for the packet. The packet move towards destn as & how they get forwarded. Due to the lack of a defined connection between source & destination the type of switching is called connectionless.

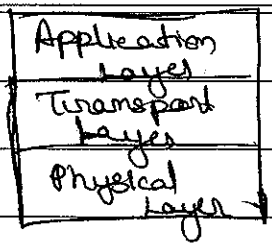
In circuit switching the entire path is dedicated to single communication for whole duration whereas in connection less packet switching no path is selected To improve on both this techniques it was decided that a path from source to destn to be ~~dedicated~~ decided but it should not be dedicated to one user but can be shared by other users.

Connection Oriented packet switching

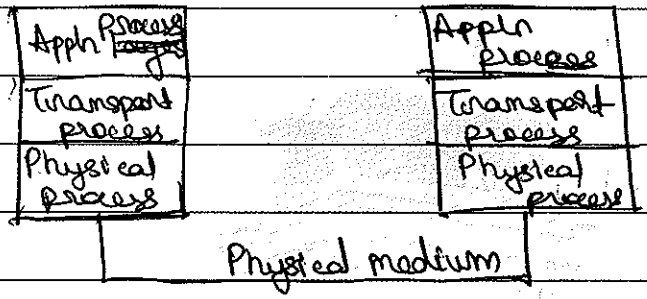
In the COPS the individual packets don't travel through the network ~~through~~ in different paths but all the packets for particular source destn pair take the same pre-selected path that is the selected connection

Chapter – 3
Communication process & layered Architecture

Communication can be visualized as a process which takes place in different steps as a function of time. The 1st & foremost is the generation of information / idea where the mind comes to picture. Idea is then conveyed to other & is represented in appropriate form. For actual communication physical media is required to convey the information. It can be represented as 3 stage communication process & is ~~placed~~ represented as 3 layers.



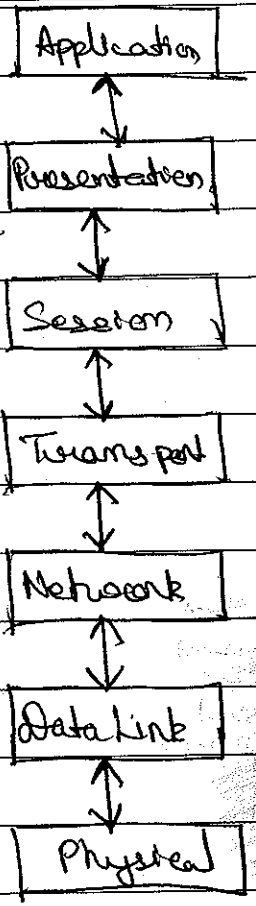
Of the two machines A has to communicate the layered process can be represented as



One of the example for layered networks is OSI model

OSI reference model

OSI model has 7 layers. OSI tells what each layer should do



Physical layer: Physical layer transmits raw bits over a communication channel.

Data link layer: Data link layer takes raw info & transform it into free of transmission errors & sends it to network layer. It accomplishes this task by having the sender break the input data up into data frames, transmit the frames sequentially & process the acknowledgement frames sent back by the receiver.

Network layer: This decides how packets are routed from source to destination. It also controls the congestion of packets (When 1 packet travels from 1 network to another to get to its destination many problems arise. Addressing used by the second network may be different & might not accept the packet. Network layer has to overcome this.

Transport layer: Basic function of transport

layer is to accept data from the session layer split it & pass it to network layer.

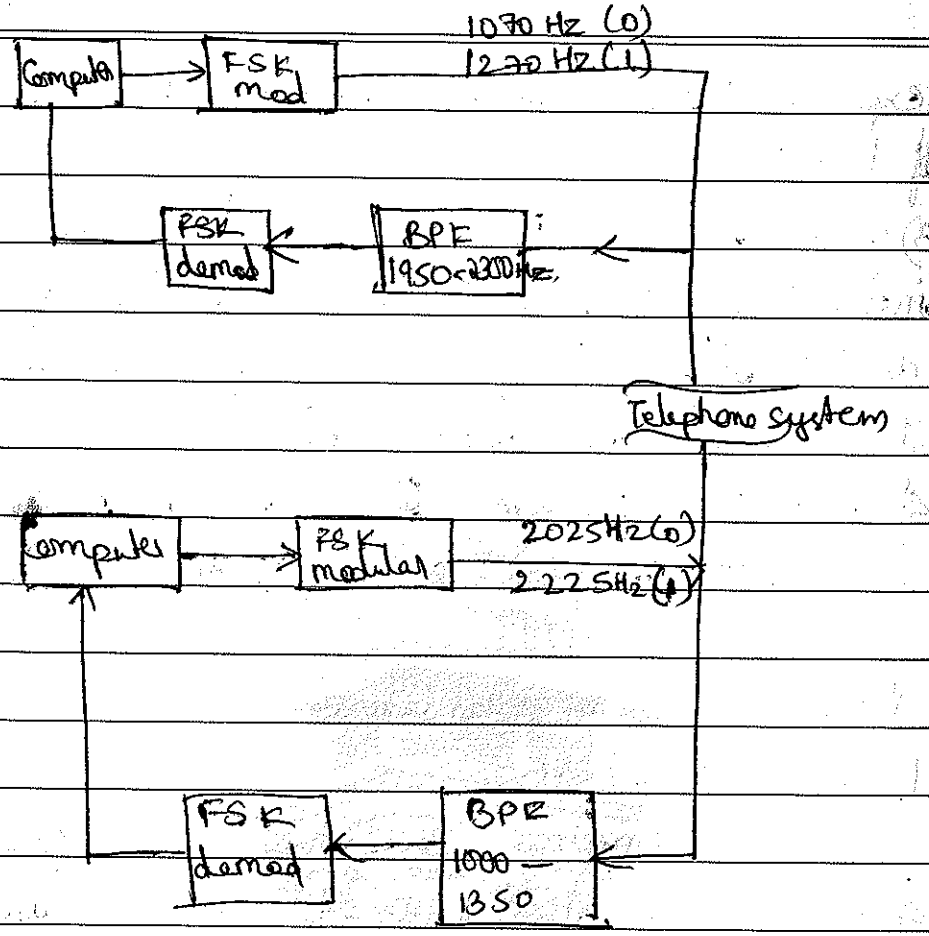
Session layer: Allows users on different machines to establish session between them. It also helps in to manage dialogue control.

Presentation layer: It is concerned with the syntax of the information transmitted.

Application layer: Its function is to transfer a file to a node.

Operation of Modem

A modem is a device containing both a modulator & a demodulator. It is used to transmit digital data from computer in form of analog signals over telephone line.



Types of modem:

1) External modem. They are connected to computer externally through a cable to serial port of computer.

2) Internal modem. These modems are placed inside the computer. They are less

expensive than external modems because of less hardware.

3) Optical modem. They use optical fiber instead of wire. The modem converts the digital signal to pulses of light to be transmitted over optical lines.

4) Short Haul Modem. It is used to transmit within a short distance.

V series Modem Standards

1) V.32 & V.32 bis
V.32 employs Quadrature Amplitude Modulation. data rate of 9600bps
It has a baud rate of 2400. V.32bis also uses QAM with a baud rate of 2400 bps.

2) V.34 bis : It provides bit rate of 33,600 bps

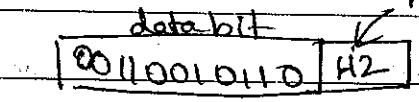
3) V.90 - It has a bit rate of 56,000 bps. It is also called as 56K modem. Uploading & downloading rates are diff.

V.92 → Uploading rate is 33.6kbps.

V.92 → They can be uploaded at a rate of 48Kbps & downloaded at 56kbps.

Function of Data link Layer

1) Header & Trailers are added containing the physical addresses of nodes & is removed upon successful delivery.
2) On LAN it decides who can send data when & has thorough Media Access Control technique.
3) Headers have bits which tell the receiver when a frame is arriving.
4) It checks frame to ensure it is free of error.

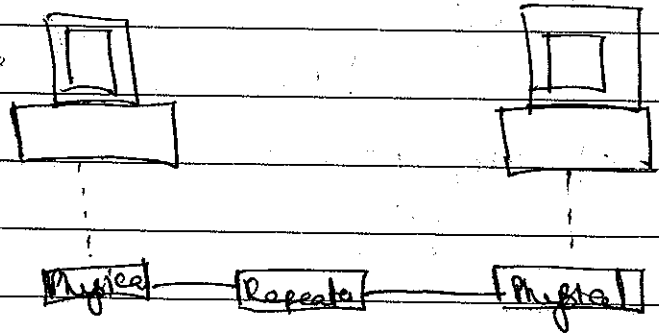


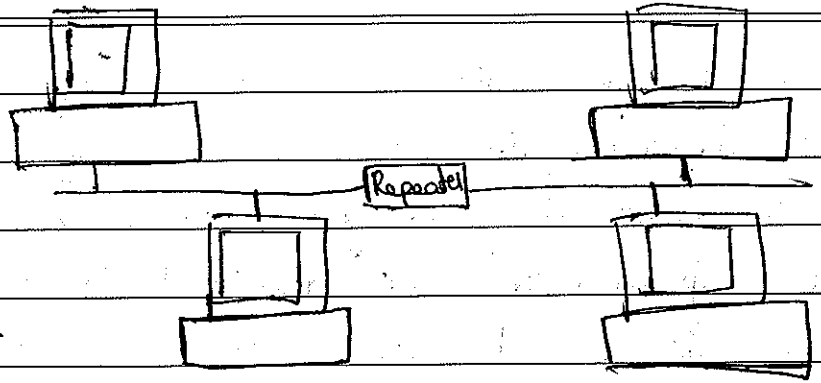
The most important responsibilities of the data link layer are flow control & error control.

Flow control: Flow control coordinates the amount of data that can be sent before receiving an acknowledgment & is one of the main function of data link layer. In most protocols flow control is a set of procedures that tells the sender how much data it can transmit. The flow of data must not be allowed to exceed the receiving capacity of receiver. The receiving device must be able to inform the sending device before these limits are reached & should request transmitting device to send fewer frames stop temporarily

Error Control: Error control is both error detection & error correction. It allows the receiver to inform the sender of any frames lost or damaged in transmission. Any time an error is detected in an exchange specified frames are retransmitted. This process is called automatic repeat request

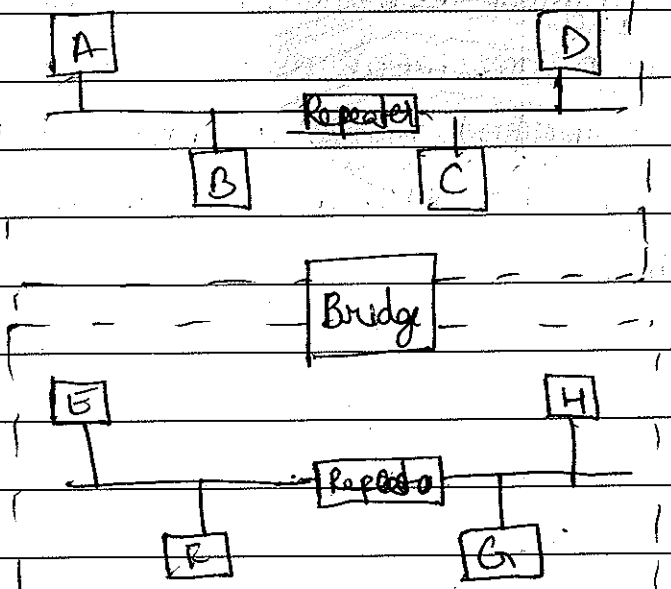
Repeaters: A repeater also called a regenerator is an electronic device which simply regenerates a signal. Signals traveling across a physical wire travel some distance before they become weak or get corrupted as they get interfered with other signals/noise. A repeater receives such a signal which is likely to become weak or corrupted & regenerate it.





Bridges:

A bridge is a computer that has its own processor memory & 2 NIC cards to connect to 2 portions of a n/w.



Router: A router operates at physical data link & network layers of OSI model. A router is termed as intelligent device. A router is useful for interconnecting 2 or more networks. These n/w can be differ in the properties such as Token rate topologies etc. Router has to determine best possible transmission path among several available.

Gateway: Gateway operates at all the seven layers of the OSI model. It is used to communicate between 2 nodes having different protocol.

To Medium access Control (MAC)

The token Ring hardware ensures that the permission for data transmission is granted to each host on the Token Ring in turn.

The hardware facilitates this coordination by using 3-byte frame called token. Token contains bit pattern that is completely different from data frame.

A host waits for token frame to arrive before sending a frame. When a host receives the token frame it knows it has exclusive access to transmission medium. It accepts it & sends its own data frame. Once data frame completes I full journey the transmitting host then sends back the token frame onto the medium. The circulating mechanism of the token frame ensures that every host is given an equal chance for data transmission. If a host has 2 or more frames to transmit it must send one frame at one time.

Addressing Mechanism

It uses 48-bit NIC address.

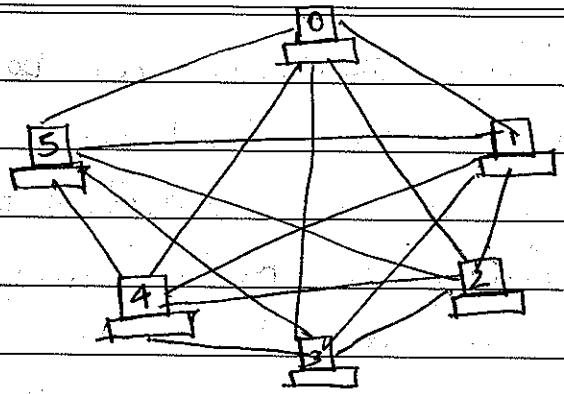
Token Ring Properties

1) It transmits data rate upto 10 Mbps.
2) It consists of twisted pair wire sections to link to their neighbours.

Chapter - 4
Local Area Network

Network topology defines how various computers or nodes are connected to one another. There are 6 basic topologies

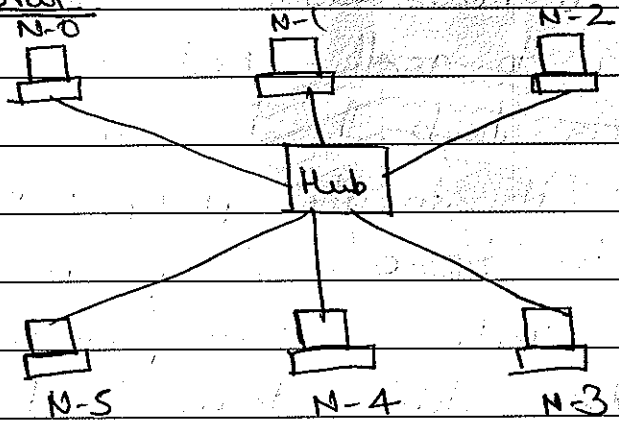
① Mesh topology: In this each node is connected to every other node by direct links. This does not have traffic congestion problems due to dedicated links. In this if one link is down the rest of the network can still continue. Fault identification is also easy. The main demerit of this scheme is cable length & consequent cost & complexity.



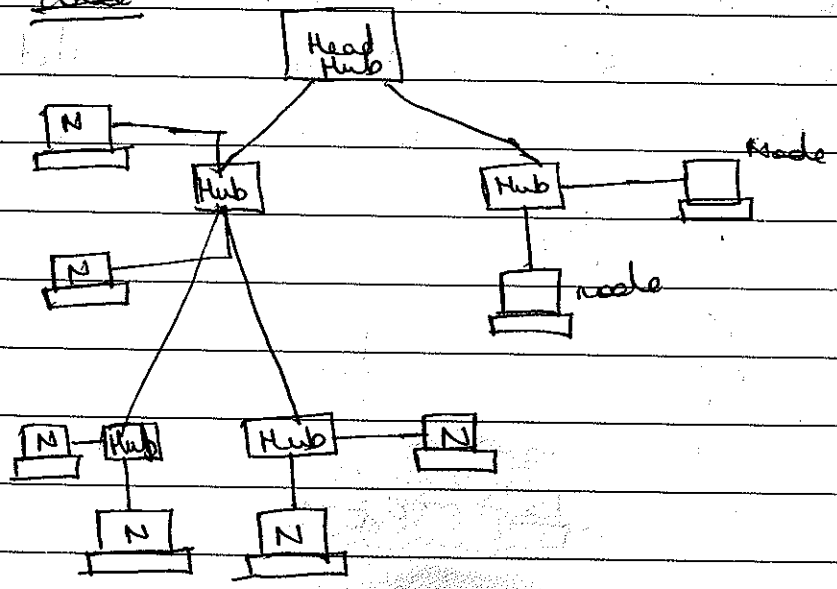
② Star topology: In this type there is a central node often called as a hub. If a node wants to send some data to another node it sends it to this hub. The hub in turn sends it to the appropriate hub. Star topology is cheaper than mesh topology. If one link is bad all others still continue functioning except that node & that link. If the hub goes down then the entire n/w becomes dysfunctional.

Tree Topology: Tree topology can be derived from the star topology. On this every node is connected to some hub. Only a few nodes are connected directly to the central hub. The central hub is called as active hub & secondary hubs are called as passive hubs.

Star:

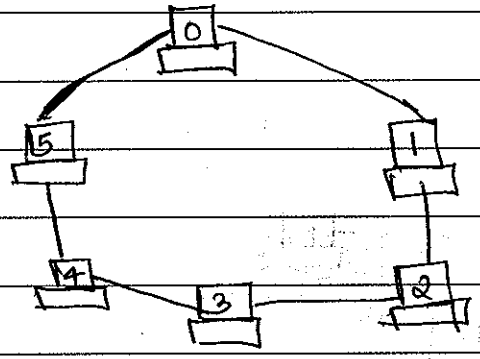


Tree:

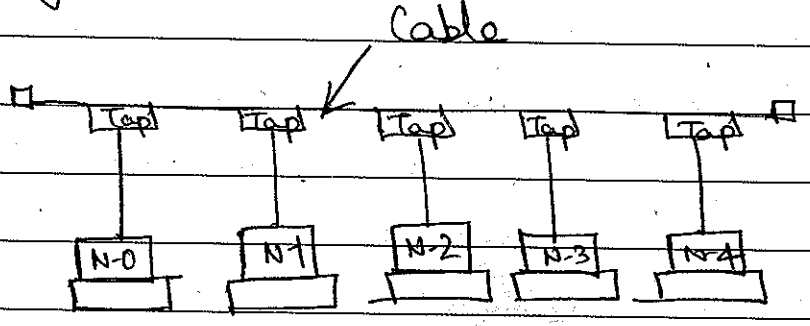


Ring Topology: In this topology each node is connected to only its 2 adjacent neighbours. If a node wants to send something to a distant node on a ring it has to go through many intermediate nodes which act like repeaters. A node not receiving any signal for a long time indicates a fault. If a node is a simple

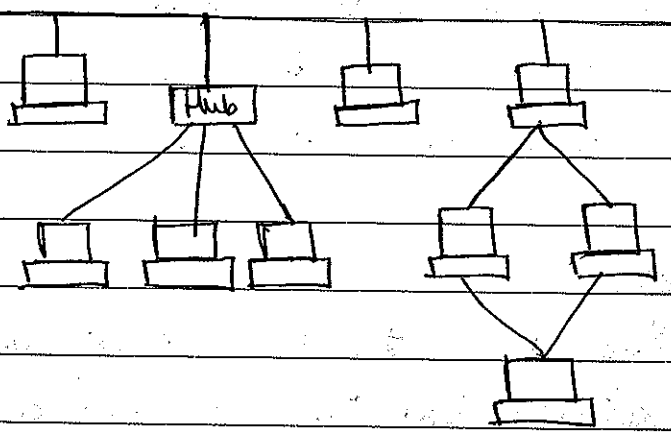
ring fails the whole ring cannot function. Another disadvantage is that traffic flows only in one direction.



Bus Topology: This uses multipoint philosophy. A long cable called bus acts as a backbone for all nodes. A node wanting to send some data to some other node pushes the data on the bus, which carries it to the other node where it is received & the same way, ~~& passengers get on~~. It uses less cables than mesh, star or tree topologies. On this fault identification is very difficult. If a portion of the bus breaks down the whole bus cannot function



6) Hybrid Topology: It uses two or more of the other topologies. Bus, star & ring topologies are used to create the hybrid topology.



Local Area Networks

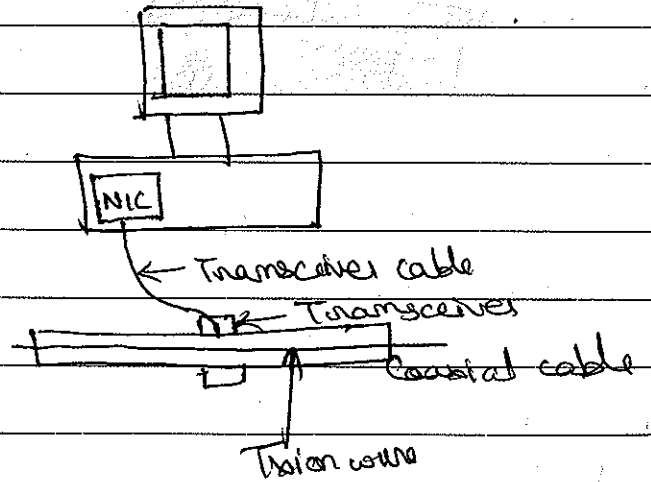
On LAN all hosts share a single transmission medium. The address in the packet or frame enables the destination host to receive that packet, while other hosts ignore it. Broadcast network can be static or dynamic

On static method each host is given a fixed time slice to send info. If host does not have anything to send that time slice is wasted.

On dynamic host can send frame at any time. If 2 host send frame at the same time frames could collide with each other.

Ethernet:

Ethernet is the name of popular packet switching LAN. Ethernet uses a single coaxial cable as the transport medium. All host in the Ethernet LAN connect to this cable at device called transceiver is used to establish the connection between a computer & the Ethernet. A small hole is made in the outer layer of the coaxial cable so that a transceiver can attach to the medium actually carrying the signals. The transceiver is responsible for sensing voltages on the cable & interpreting the signals.



NIC (Network Interface Card) controls

the operation of its transceiver using the network software inside the host. The transceiver does not connect the host directly. It connects to a Network Interface Card; a small card plugged on the motherboard of the host which functions like small computer. It has small CPU, memory & a limited instruction set. It performs all the network related functions. Each NIC bears a unique hardware address or physical address that identifies host uniquely. The hardware address is guaranteed to be unique all over the world.

Ethernet Properties:

a) Broadcast n/w: Ethernet is a broadcast network because the transceiver of every host receives every transmission from any host on the network. It transceiver does not have any intelligence built in. It simply accepts all the bits of a frame travelling across the Ethernet & hands them over to NIC. It is the NIC which decides if the frame is of any relevance to itself by matching the destination address field in the frame with its own address & accordingly either accepts or ignores the frame.

b) Best effort delivery: The hardware does not provide any information to the source of the sending host if the frame sent by it has successfully reached the destination.

c) Decentralized access control: The control to the transmission cable is distributed. In case of Ethernet there is no single centralized authority that dictates if a host can transmit data.

Carrier Sense Multiple access with Collision Detect (CSMA/CD)

On CSMA/CD multiple hosts can access the Ethernet bus simultaneously through their transceivers and can determine if it is idle by looking for the presence/absence of a carrier wave on the bus. For this reason it is called Carrier Sense Multiple Access.

When the transceiver of a host begins transmission on the Ethernet the signal does not immediately reach all the parts of n/w. It travels at speed of about 80% of the speed of light across the Ethernet. Until the signal reaches another host that host continues to believe that the cable is idle. It is possible that 2 transceivers believe that the Ethernet is free for transmission & can transmit data almost exactly at same time. leading to intermingling of electrical signals. Such incidents are termed as collisions which the transceivers of both the sending hosts can detect.

The transceiver informs NIC about it. NIC stops further transmission & waits for some time before it asks the transceiver to retransmit the data. The NIC of other node also performs the same procedure. The waiting time is followed by a Ethernet standard called as binary exponential backoff policy whereby a sender waits for a random time after a 1st collision, twice if retransmission also results in collision 4 times the next round.

Ethernet Addresses

Ethernet has 48 bit long physical address called Ethernet address. An ethernet address is always unique & is handcoded on NIC.

Ethernet frame format:

The Ethernet is a data link layer connection between hosts. Unit of data exchanged by hosts over the Ethernet is called as frame. An Ethernet has a format as shown below

Preamble	Dest Address	Source Add	Frame type	Frame Data	CRC
8 bytes	6 bytes	6 bytes	2 bytes	64-1500 bytes	4 bytes

Preamble: The preamble contains 8 bytes or 64 bits of alternating 0s & 1s to help the receiving hosts to synchronize.

Destination address: The 6 byte or 48 bit address of the destination to which the frame is addressed is contained in this field. This is the hardware NIC address.

Source address: The NIC of the sending host inserts the hardware NIC address of the sender in this 6 byte or 48 bit field.

Frame type: This field identifies the type of data carried in the frame.

Frame data: This field contains the actual data of the frame of variable length

CRC: The 4 byte or 32 bit field helps the dest NIC to detect transmission errors.

Token Frame

All hosts on a Token Ring share the same physical medium just as the hosts on Ethernet. If a host on a ring wants to transmit data it cannot send it immediately. It must wait for the permission to do so. Once a host gets the permission for data transmission, no other host would be allowed to transmit data at same time. A host has exclusive control over the Token medium when it is about to transmit data.

The sending computer transmits a frame which travels across the ring. This means each host on the ring has to accept it, check the destn address & if it is not meant for it, it should forward it along. Every host forwards it to next host, so the frame actually comes back to the sender.

Token Ring Frame

Preamble	Destn address	Source Address	Frame Data	CRC	ED	FS
3 bytes	6 bytes	6 bytes	Upto 4500 bytes	4 bytes	1 byte	1 byte

Preamble: It is used for synchronization purpose. It also indicates that it is a data frame.

Destination address: The 6 byte or 48 bit address of the NIC.

Source address: The NIC of the sending host adds the NIC address of the sender to this 6-byte or 48 bit field

Frame data: This field contains the actual data of the frame which is of variable length.

CRC: It is 32 bit field which helps the source & destination NIC to detect transmission errors.

(End Delimiter)

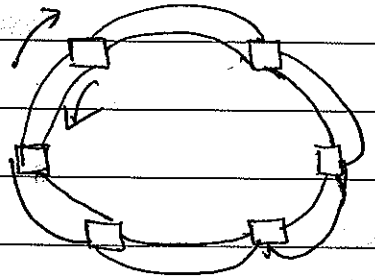
ED: This one byte field signifies that the sender's data & control information ends here.

FS (Frame Status): It arrives after CRC has been checked & it is an acknowledgement.

Fiber Distributed Data Interface (FDDI)

FDDI n/w architecture & a LAN protocol. It supports data transmission rates of up to 100 Mbps & is an alternative to Ethernet & Token Ring architectures. FDDI uses glass fibers for data transmission as mentioned before & encodes data bits in the form of pulses of light.

Operation of FDDI: It is similar to to Token Ring with one difference that it employs 2 independent rings to connect to every host.



Normally FDDI uses only 1 ring for data transmission.

Self-Healing Mechanism: When a n/w error occurs or a host is down the NIC of a host realizes that it cannot communicate with it neighbouring host. On such case the NIC uses the second ring which is used as a backup for such failures for data transmission. This is called loopback.

FDDI frame:

Preamble	Destn address	Source Address	Frame data	CRC	ED	FS
2 bytes	6 bytes	6 bytes	Upto 4500 bytes	4 bytes	1 byte	1 byte

Preamble: It is used for synchronization purpose.

Destination address: The 6 byte NIC of destn to which frame is addressed

Source address: NIC of the sending host adds the NIC address of the sender.

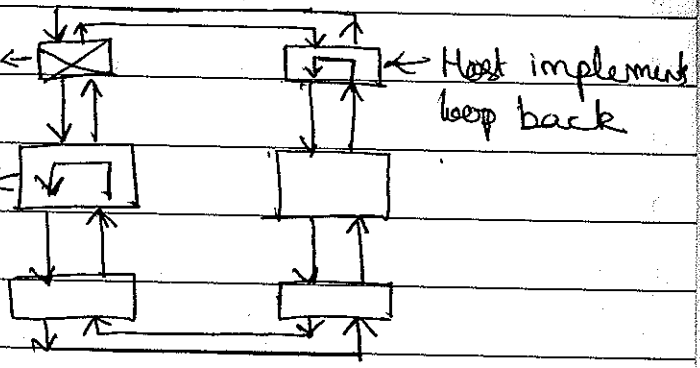
Frame data: This field contains the actual data of the frame.

CRC: This 32 bit field helps the source & destination NIC to detect transmission errors.

ED: It signifies that the sender's data & control info ends here.

FS: This 1 byte field is the last in data frame. The receiver sets it when it receives the frame.

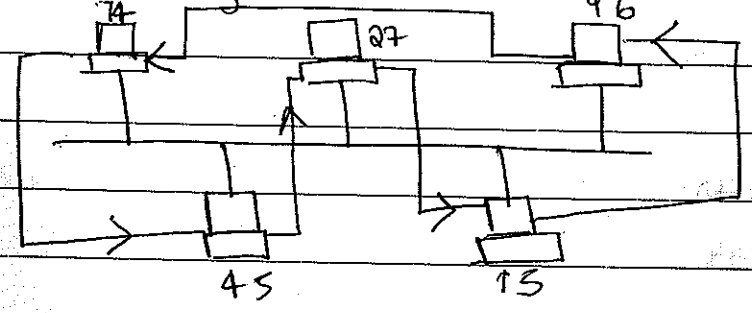
Self Healing Mechanism Diagram



IEEE 802.4 - Token Bus

Token Bus combines features of Ethernet & Token Ring. It combines the physical configuration combination of Ethernet (a bus topology) & collision free deterministic feature of Token ring. The logical ring is formed based on the physical addresses of the stations in descending order.

Eg:

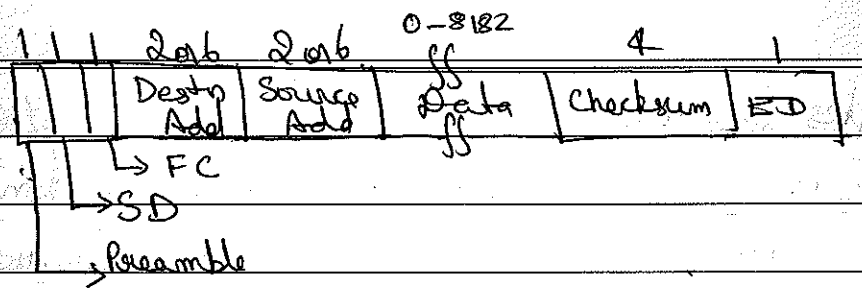


To control access to the shared medium a small token frame circulates from station to station in logical ring. If a station has data frames to send it keeps the token & sends its data frames. To prevent domination of the medium by one station the protocol defines a specified period of time that each station can hold the token.

Token Bus Maintenance

Token bus protocol depends on the maintenance of the logical ring & controlling of token. For ring management the Token Bus uses seven special frames. for eg: claim_token, solicit_successor_2, who_follows, resolve_contention, token, set_successor.

Token Bus Frame Structure



Preamble: It consists of 1 byte pattern to synchronize the sender & receiver.

Start Delimiter: It is used to alert the receiving station to the arrival of a frame

Frame Control: Frame Control field is used to specify frame type. The allowed types include token passing & various ring maintenance frames including.

Destination address: The 2 byte or 6 byte physical address of the NIC in the destn to which the frame is addressed is contained in this field.

Source address: The NIC of the sending host adds 2 byte or 6 byte NIC address of the sender to this field.

Data: The data field is made up of 8182

bytes long.

Checksum: The checksum field is 4 bytes long & contains a CRC error detection sequence

End Delimiter: The end delimiter field is used to alert the receiving station to the termination of a frame.

IEEE 802.5: Token Ring Maintenance

Each token ring has a monitor station that oversees the ring. Every station has the capability of becoming the monitor. Monitor responsibilities include the following: whether seeing that the token is not lost, taken action when the ring breaks etc.

Token ring: describes 3 frame formats

1. Data frame
2. Token frame
3. Abort frame

Data Frame:

Preamble	Destn	Source	Frame Data	CRC	ED	FS
3 bytes	6 bytes	6 bytes	4500 bytes	4 bytes	1 byte	1 byte

Preamble: It is used for synchronization purpose. It contains 3 sub-field each consisting 1 byte. It also indicates it is a data frame or token or a abort frame.

Destination address: The 6 byte address of the NIC in the destn to which the frame is addressed in this field

Source address: It contains NIC address of sender

Frame Data: It contains data of the frame

CRC: The 32 bit is used to detect error during transmission.

ED: It signifies that senders data & control info ends here.

FS: This 1 byte arrives after CRC has been checked.

Token frame:

SD	Access Control	End Delimita
1byte	1byte	1byte

SD: It signifies to a host that a frame is coming

Access Control: It indicates to the host that arriving frame is token frame.

ED: It indicates it is end of token frame

Abort frame:

SD	ED
1byte	1byte

It is used by a sender to abort an ongoing transmission.

SD: It signifies host frame is coming

ED: signifies host end of the abort frame

Wireless LAN:

Wireless LAN: A wireless LAN is a LAN that uses infrared light waves or radio waves instead of copper wires or optical fibers. Distance of coverage depends on the transmitter & sensitivity of receivers.

WLAN employs 802.11 standard.

IEEE 802.11 standard specifies 2 kinds of services:

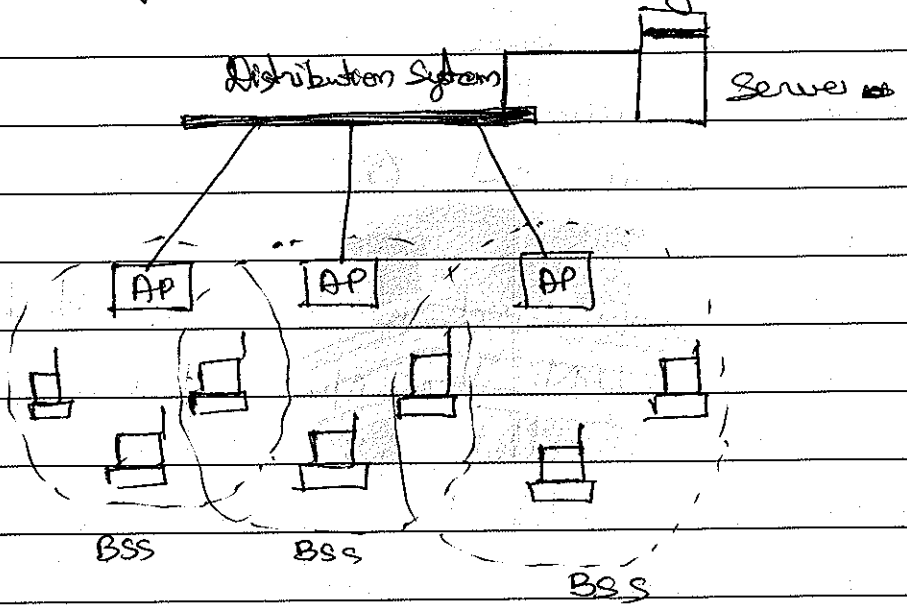
① Basic service set ② Extended service set.

Basic service set is the building block of a wireless LAN. The n/w configuration with 1 cell is called BSS. AP is a central base station for a group of users within a basic geographic area. It forms bridge between wireless equipment & the wired IEEE LAN.

Extended Service Set: An extended service set is made up of 2 more BSS with AP.

Ad-Hoc network: BSS without an AP cannot send data to other BSS. It is called ad-hoc network or peer to peer n/w.

eAppln: Used at a convention centes
b) conference room to exchange data



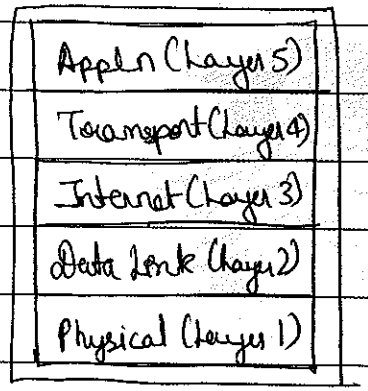
802.11 WLAN architecture

Chapter-5
Metropolitan Area Network

Chapter-6
TCP/IP

The transmission Control Protocol / Internet Protocol forms the basis of Internet working. TCP/IP was developed before OSI.

TCP/IP model



Physical layer:

This layer deals with raw data i.e voltages.

Data link layer:

The data link layer is also very similar to other network models. This covers MAC strategies i.e who can send data & when. It also deals with frame format.

Network layer:

It deals with the format of datagrams as defined by Internet protocol (IP) & also about the mechanism of forwarding datagrams from source computer to final destn. This layer is also responsible for actual routing of datagrams.

Transport layer: There are 2 main protocols in this layer Transmission Control Protocol (TCP) & User Datagram Protocol. TCP ensures that the comms between the sender & the receiver is reliable error-free & in sequence. The IP layer sends individual datagrams through

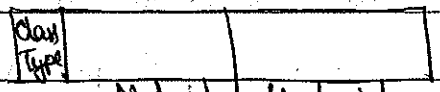
various routers choosing a path for each datagram each time. IP does not check the CRC for the data in each datagram. At the destination the TCP s/w is responsible for checking the CRC, detecting any errors & report them & acknowledging. UDP is also used in this layer. TCP is more reliable compared with UDP. UDP is used to send voice or video & TCP for sending data such as bank transactions.

Application Layer: Application layer allows an end user to run various applications on the internet. These applications are File Transfer Protocol (FTP), email, World wide web.

Internet address

It consists of 4 bytes (32 bits)

It consists of 3 fields (i) class type (ii) net id (iii) host id. These parts are of varying length



Physical address

To identify a computer over the internet they use physical addressing for each computer. Physical address is also called as hardware address. There are 3 methods to assign the hardware address to a computer

1) Static address: On this physical address is hard coded in Network Interface Card of the computer. This address does not change

2) Configurable address: The physical address is configured inside a computer when it is first installed at a site.

3) Dynamic address: Every time a computer boots a server computer

dynamically assigns it a physical address. Physical address keeps on changing every time a computer is switched off & on. A pool of free physical addresses are used to identify free addresses out of them & one such free address is assigned to the newly booting computer.

Internet address (continued).

IP protocol defines & specifies that each computer on the Internet be assigned a unique 32-bit no. called as Internet protocol address. Each datagram consists of 32 bit address of sender & destination. The 'network id' denotes the physical n/w to which the computer is attached. The host id identifies an individual computer on that n/w. Each physical n/w on the Internet is assigned a unique n/w number & assigning n/w numbers must be done at a global level as no 2 n/w nos across the Internet can be same. The assignment of host nos can be done locally. Within a n/w no 2 hosts can have the same host no.

Classes of IP addresses

The IP address space is divided into 3 primary classes named A, B, C. In each of these classes, a different no of bits are reserved for the n/w no & the host number portions of an IP address.

Class A allows 7 bits for n/w no & 24 bits for host no. Thus allowing fewer n/w to have a large no of hosts.

Class C reserves 21 bits for the n/w number & just 8 bits for the host no. Thus useful for a large no of networks that

have smaller no of hosts.

In addition there are 2 more classes D & E which serve as special purpose. Class D is used for multicasting. It is used when a single message is to be sent to a group of computers. Class E is not used as of now. It is reserved for future use.

Class A → | 0 | Nw Id | Host id |

Class B- | 1 | 0 | Nw Id | Host id |

Class C → | 1 | 1 | 0 | Nw Id | Host Id |

Class D → | 1 | 1 | 1 | 0 | Multicast address |

Class E → | 1 | 1 | 1 | 1 | 0 | Reserved for future use |