Unit - 3

Multiple accer protocol and network :-

Network → Note :- Network theory I unit ki

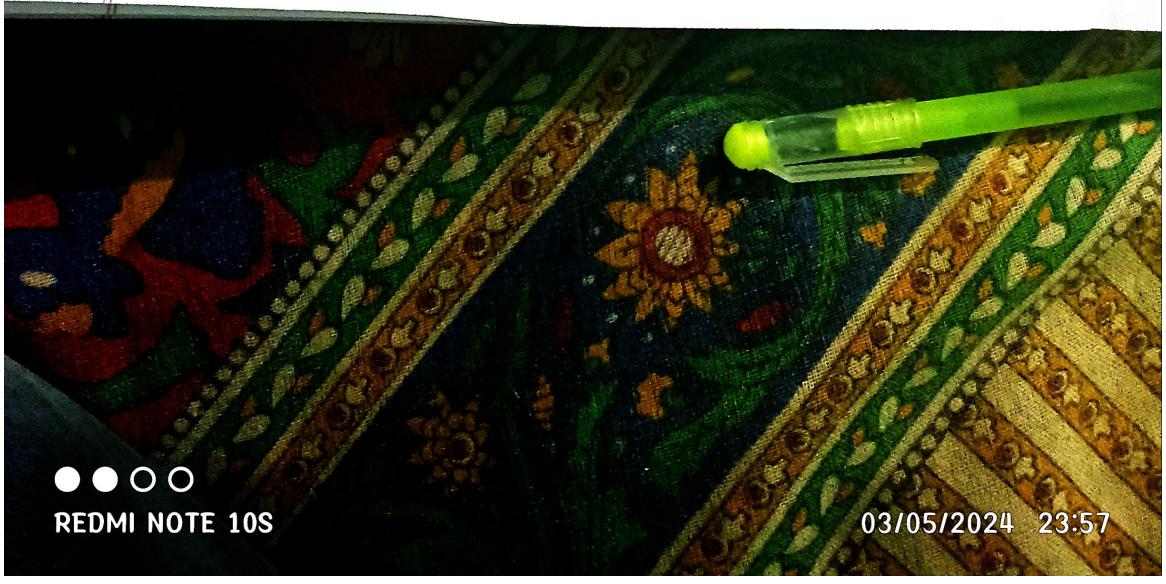
Protocol :- In networking, a protocol is a standardized a set of rules for formatting and processing data. Protocols enable computers to communicate with one another.

TCP/IP :- The internet protocol (IP) and transmission control protocol (TCP) are together known as TCP/IP protocol. TCP/IP offers a simple naming and addressing scheme whereby different resources on internet can be easily located. Information on internet is carried in "packets". The IP protocol is used to put a message into a "packet". Each packet has the address of the sender and the recipients address. These addresses are known as the IP addresses using the TCP protocol, a single large message is divided into a sequence of packets and each is put into an IP packet.

2 File Transfer protocol:- Many network systems provide computers with the ability to access files on remote machines. Some designers provide remote file access to lower overall cost. In such architecture, a single centralized file server provides secondary storage for a set of inexpensive computers that have no local disk storage, Eg:- the diskless machines can be portable devices used for chores such as inventory.

3 User datagram protocol:- The user datagram protocol is a very simple protocol. It adds little to the basic functionality of I.P. Like IP, it is an unreliable, connectionless protocol, you do not need to establish a connection with a host before exchanging data with it using UDP, and there is no mechanism for ensuring that data sent is received.

4 Hypertext transfer protocol:- The hypertext transfer (HTTP) is the foundation of world wide web, and is used to load webpages using hypertext link. HTTP is an application layer protocol, designed to transfer information between networked 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.

5. Simple mail transfer protocol:-

SMTP is a application layer protocol of TCP/IP model. SMTP transfer message from sender's mail servers to the recipients mail servers. SMTP interacts with the local mail system and not the user. SMTP uses a TCP packet on port 25 to transfer email reliably from client to server. E-mail is temporarily stored on the local and eventually transferred directly to receiving server.

6. Unix-to-Unix copy protocol:-

UUCP is derived from Unix-to Unix copy protocol. It is a standard UNIX utility that manages the transmission of information between UNIX systems, using serial connections and regular telephone lines. The communications package was developed at Bell laboratory by Mike Lesk in the mid-1970s for serial

communications between in-house UNIX systems.

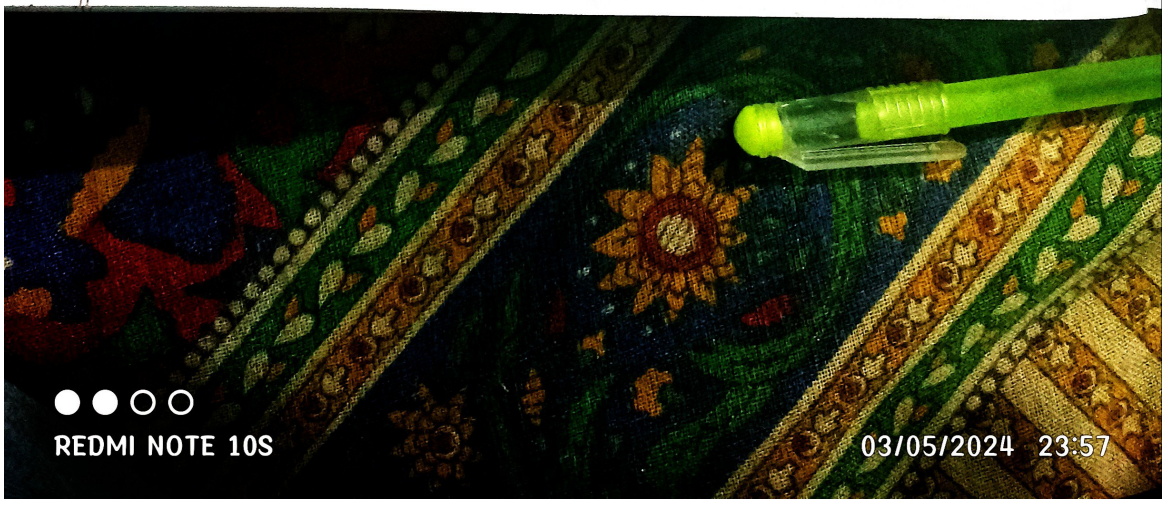
7. Simple Network Management protocol :-

Simple Network Management protocol (SNMP) is an application-layer protocol for monitoring and managing network devices on a local area network (LAN) or wide area network (WAN).

The purpose of SNMP is to provide network devices, such as routers, servers and printers, with a common language for sharing information with a network management system (NMS).

8. POP ~~protocol~~

The POP ~~protocol~~ stands for Post office protocol. As we know that SMTP is used as a message transfer agent. When the message is sent, then SMTP is used to deliver the message from the client to the server and then to the recipient server. But the message is sent from the recipient server to the actual server with the help of the message access agent. The message access agent contains two types of protocols,



i.e. POP and IMAP

9. MIME protocol :-

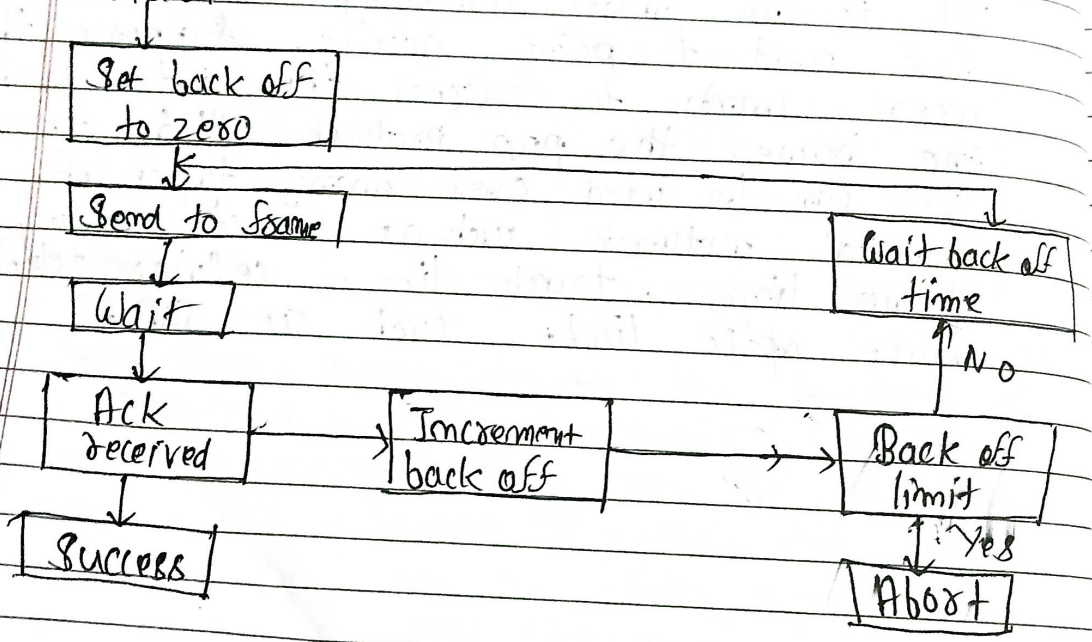
MIME stands for multipurpose Internet mail extensions. It is used to extend the capabilities of Internet e-mail protocols such as SMTP. The MIME protocol allows the user to exchange various types of digital content such as pictures, audio, video and various types of documents and files in the e-mail.

10. PPP protocol :-

The PPP stands for point-to-point protocol. It is the most commonly used protocol for point-to-point access. Suppose the user wants to access the internet from the home, the ppp protocol will be used. It can be used over many types of physical network such as serial cable, phone line, trunk line, cellular telephone, fibre optic links such as SONET.

ALOHA :-

In a system when multiple users try to send messages to other stations through a common broadcast channel, random access or contention techniques are used. Random access means there is no definite or scheduled time for any station to transmit. This scheme is simplest possible and it is asynchronous because there is no co-ordination among users. The basic idea of ALOHA system is applicable to any system in which uncoordinated users are competing for the use of a single shared channel.

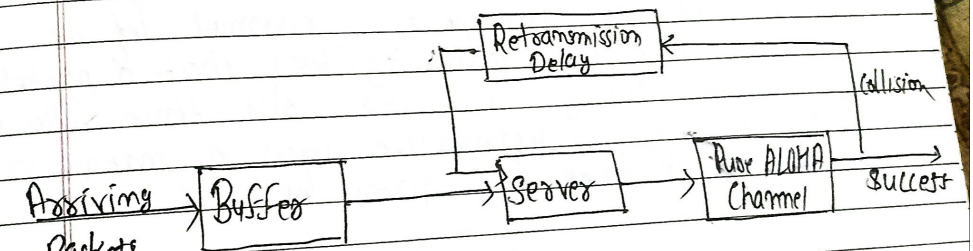


There are two versions of ALOHA system

1) Pure ALOHA
2) Slotted ALOHA

1) Pure ALOHA:

A station can transmit whenever it has data to send. To determine whether a transmission was successful, a sender waits for an acknowledgement from the receiver for a time period. If no acknowledgement is received, the message will be sent again. If a station starts to transmit when another transmission is already in progress, collisions will occur. A mechanism to detect the collision is established. Message are sent in the form of packet. Each packet contains parity bits for error detection.



⇒ Throughput of pure ALOHA channel:-

1) Throughput : The throughput S is defined as average successful traffic transmitted between stations per unit time. The unit of time is slot-time, which is the time required to transmit a frame.

2) Offered traffic : The offered traffic is the average number of packets per slot time which are presented to the network for transmissions by users. It is denoted by G. The throughout is expressed in terms of offered load or traffic G. Practically G can have any value between 0 to infinity.

3) Channel capacity :- The maximum achievable throughout for a particular type of access scheme is called the capacity of the channel.

To find the throughout of channel, let us assume that the probability (P_k) that k packets generated during a given slot-time follows a poisson's distribution with a mean G per packet time is given by

$$P_k = \frac{G_k \cdot e^{-G}}{k!}$$

The throughput S is then just the offered load G times the probability of a transmission being successful.

$\therefore S = GP_0$

where P_0 = probability that a packet does not suffer a collision

The probability of no other traffic being initiated during the entire vulnerable period is thus given by

$P_0 = e^{-2G}$

From equation

$S = G \cdot e^{-2G}$

The maximum throughput occurs at $G = 0.5$

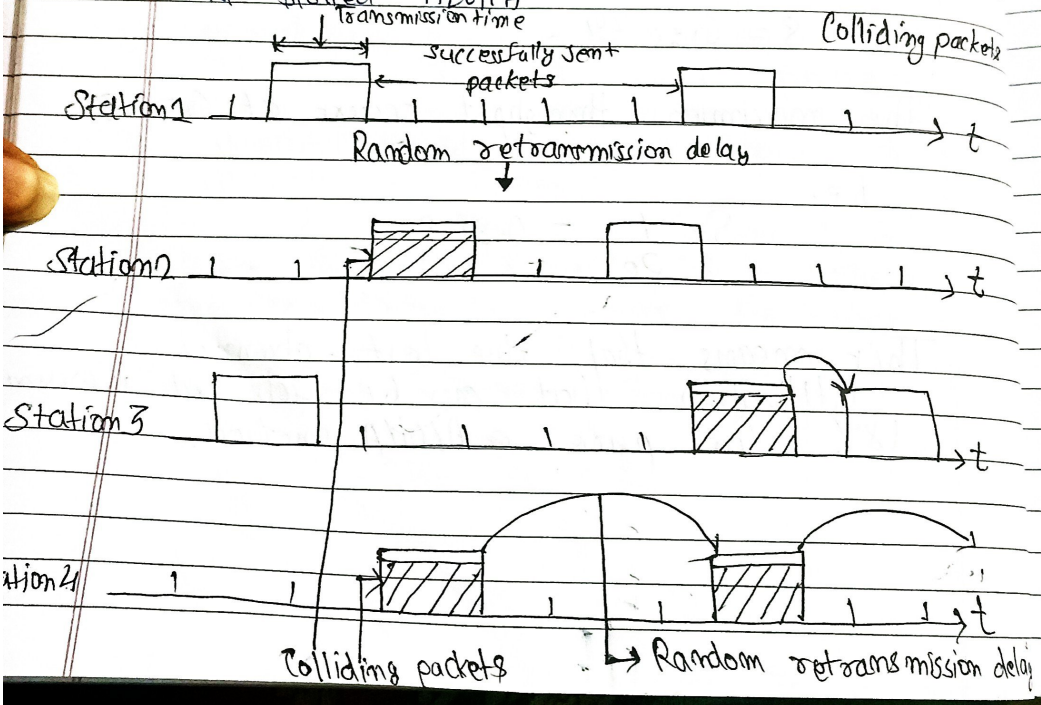
i.e.

$S = \frac{1}{2e} = 0.368$

This means that the best channel utilization that can be achieved is around 18% for pure ALOHA method.

2) Slotted ALOHA

In slotted ALOHA, the channel time is divided into time slots and the stations are allowed to transmit at specific instance of time. These time slots are exactly equal to the packet transmission time. All users are then synchronized to these time slots, so that whenever a user generates a packet it must synchronize exactly with the next possible channel slot. Consequently the wasted time to collisions can be reduced to one packet time or vulnerable period is reduced to half. Transmission attempts for four network user and random retransmission delays for colliding packets in slotted ALOHA



- Throughput of slotted ALOHA Channel:

In slotted ALOHA, the packets arrive in a synchronized fashion. The probability of single transmission during a slot time is

$$P_0 = e^{-G}$$

From equation (12.3.2)

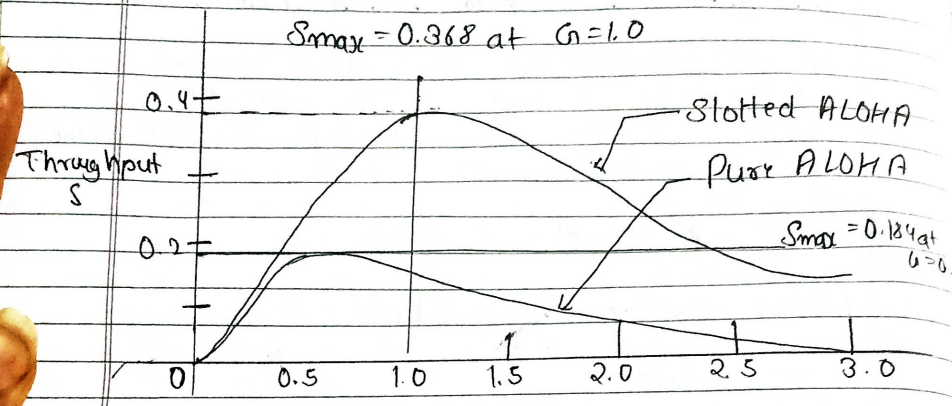
$$S = G.e^{-G}$$

The maximum throughput occurs at $G = 1$,

i.e, $$S = \frac{1}{e} = 0.368$$

which is twice that of pure ALOHA. This means that the best channel utilization that can be achieved is around 37%.

The relation between the offered traffic and the throughput is shown



Comparision of the throughput as a function of offered load for pure and slotted ALOHA

Example

Ans :

- Pros & Cons of Slotted ALOHA

Pros

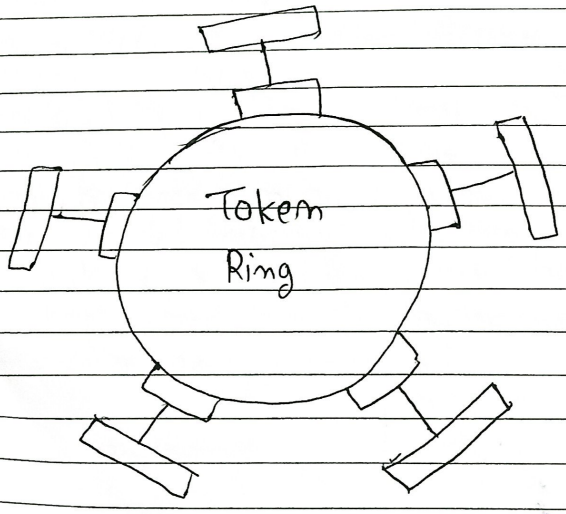
1. Single active node can continuously transmit at full rate of channel.
2. Highly decentralized, each node independently decider when to retransmit.
3. Simple to implement.

Cons

1. Collisions waste slots
2. Idle slots

★ Token Ring (IEEE 802.5):

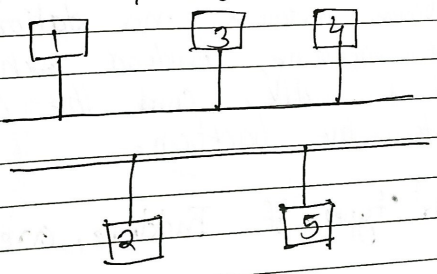
In a token ring a special bit pattern called the token circulates around the ring whenever all stations are idle. When a station transmit. It breaks the ring and inserts its own frame with destination and source address. When the frame eventually returns to the originating station after completing the round the station removes the frame and closes the ring because there is only one token only one station can transmit at a given instant thus solving the channel access problem.

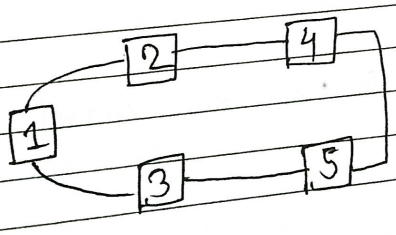


★ IEEE 802.4 (Token bus):-

IEEE 802.4 describes a token bus LAN standard. In token passing method stations connected on a bus are arranged in a logical ring. When the logical ring is initiated the highest numbered station may send the first frame. After this it passes permission to its immediate neighbour by sending a special control frame called a token. The token propagates around the logical ring with only the token holder being permitted to transmit frame since only one station at a time holds the token collisions do not occur. There is no relation between the physical location of the station on the bus and its logical sequence number.

Physical topology





Logical sequence of token passing

* Back- bone networks :-

Backbone is most important part of a system which provides the control support to the reset system, for ex :- backbone of a human body that balance and hold all the body parts. Similarly in Computer networks containing a high capacity connectivity infrastructure that backbone to the different part of the network.

Actually a backbone network allows multiple LAN's to get connected in a backbone network, not a single - station is directly connected to the backbone but the stations are part of LAN, and backbone connect those LANs.

Backbone LAN: The backbone network allows several LANs to be connected. In the backbone network, no station is directly connected with backbone instead each station is a part of a LAN, and the LANs are connected to the backbone.

There are four types of Backbone, are as follows:

1) Bus backbone
2) Star backbone
3) Interconnection of remote control.

1) Bus

In back

2) St

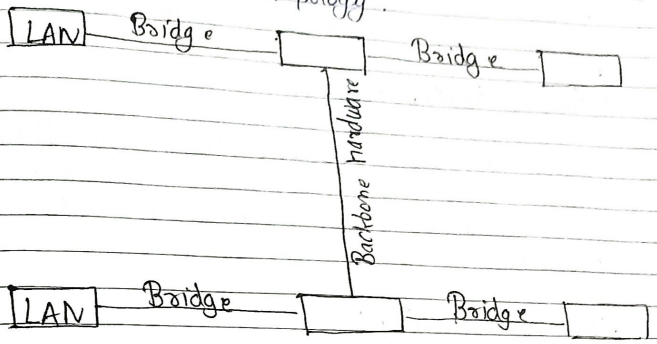
3)

REDMI NOTE 10S

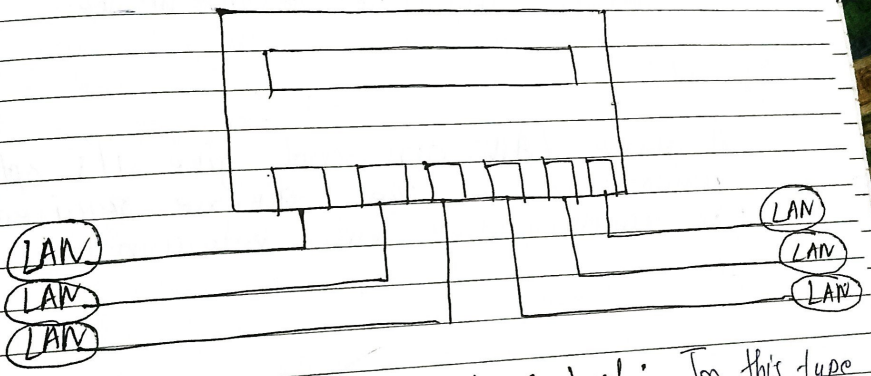
03/05/2024 23:58

1) Bus Backbone :

In bus backbone the topology used for the backbone is bus topology.



2) Star Backbone : The topology of this backbone is star topology.



3) Interconnection of remote control : In this type of backbone network the connection are done through the bridge called remote bridges which acts as connecting devices in connect LANs as point-

to point network link

=> It is possible to develop a single LAN for this purpose but practically this scheme faces the following drawbacks:

1) Poor Reliability:

With a single LAN, the reliability will be poor since a service interruption even for a short duration can cause major problem to the user.

2) Cost: Capacity:

There is a possibility that a single LAN may be saturated due to increase in number of devices beyond a certain number.

3) Cost:

A single LAN can not give its optimum performance for the diverse requirements of communication and interconnection

CSMA/CD [Carrier sense multiple access / Collision Detection]

CSMA/CD is the most commonly used protocol for LANs. CSMA/CD specification were developed jointly by Digital equipment corporation (DEC), Intel and Xerox. This network is called as Ethernet. The basic protocol is that, a station with a message to send must monitor the channel to see if any other station is sending. If another station is sending, the second station must wait or defer, until the sending station has finished. Then it may sends its message.

These three protocols are:-

1) Non persistent CSMA
2) 1- persistent CSMA
3) P- persistent CSMA

1) Non- persistent CSMA: In non- persistence CSMA when a station is having a packet (frame) to transmit and finds that fixed ~~interval~~ of ~~time~~ that the channel is bury, it backs off for a fixed interval of time. It then checks the channel again and if the channel is free then it transmits.

2) 1- persistent CSMA : Any station wishing to transmit monitors the channel continuously until the channel is idle and then transmits immediately with probability one, hence the name 1- persistent.

3) P- persistent CSMA : To reduce the probability of collision in 1- persistent CSMA, not all the waiting station are allowed to transmit immediately, after the channel is idle.

ETHERNET

Both internet and ATM were designed for wide area networking. But in many applications, a large number of computers are to be connected to each other. For this the local area network (LAN) was introduced. The most popular LAN is called Ethernet. It can operate at 10 Mbps or 1000 Mbps or above.

In this section we are going to discuss three generations of Ethernet.

- Traditional Ethernet (10 Mbps)
- Fast Ethernet (100 Mbps)
- Gigabit Ethernet (1000 Mbps)

Traditional Ethernet was created in 1976 and has a data rate of 10Mbps. The fast Ethernet is its next version and has a data rate of 100 Mbps. The Gigabit Ethernet operates at the data rate of 1000 Mbps.

- Traditional Ethernet:-

The traditional Ethernet is the oldest version of Ethernet created in 1976 which is designed to operate at 10Mbps. The access to the network by a device is through the CDMA/CD and the media are shared between all the stations.

- Fast Ethernet:-

For the fast ethernet the bit time reduces from 100 msec to 10 msec. All fast ethernet use hub in place of multidrop cables or BNC connectors, also special category wires are used, generally a category-3 or category-5 twisted pair wires are used.

Network adapters

A network card or network adapter or LAN adapter is a piece of computer hardware designed to allow computers to communicate over a computer network. It is both an OSI layer (Physical layer) and layer 2 (data link layer) device, as it provides physical access to a networking medium and provides a low-level addressing system through the use of MAC addresses.

Although other network technologies exist, Ethernet has achieved near ubiquity since the mid-1990s. Every ethernet network adapter card has a unique 48-bit serial number called a MAC address, which is stored in ROM carried on the card. This is accomplished by the institute of electrical and electronics engineers (IEEE)

Network interface card (NIC)

Network interface cards, also called as network adapters, are peripheral cards that plug into motherhood of your computer and into network cable. Every computer on a network communicates with other through this network adapter.

Usually NIC

The in comp received connecti

It address Ethernet assigne

Functio

1) NIC building by

2) NIC layer

3) The and recei

4) NIC the serio poral

Usually NIC, is a separate today integrate NIC into a motherboard design.

The convert data from the form stored in computer to the form transmitted or received on cable and provide a physical connection to the network.

It forms data frames inserting it's own address and destination card's address. Ethernet adapter addresser are permanently assigned when it is made at factory.

Functions of NIC :-

1) NIC and its drivers are responsible for building the frames around the data generated by network layer protocol.

2) NIC converts binary data generated by network layer into electrical signals.

3) The main function of NIC is to generated and transmit signals over network and receiver incoming signals.

4) NIC is responsible for conversion between the two types of transmission (parallel to serial for sending data and serial to parallel for receiving data).

Types of NIC :-

NIC are categorised as follows depending upon different criteria.

1) Based on expansion slots : Depending upon what type of bus or expansion slot your PC has, NIC can be:

a) ISA
b) EISA
c) PCI
d) PCMCIA (for laptop PC)

eg. PCI Token Ring, ISA ethernet

2) Based on speed :-

a) 10 Mbps
b) 100 Mbps
c) 10/100 Mbps Autosensing

eg. Ethesfast (speed 10/100 Mbps)

3) Based on Network technology :-

a) Ethernet
b) Token Ring
c) FDDI

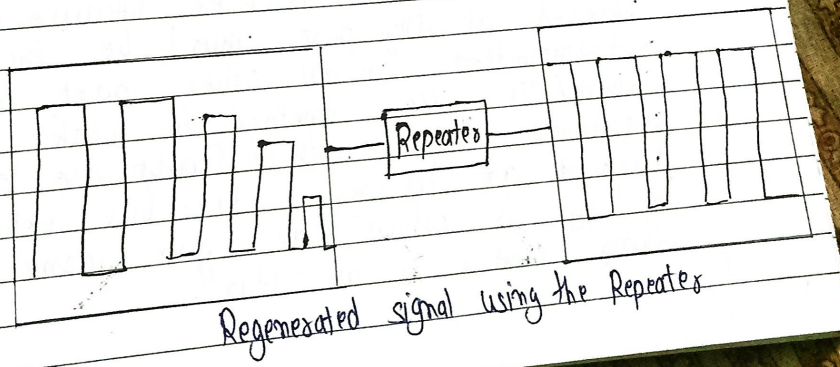
eg. PCI Token Ring.

Repeaters :-

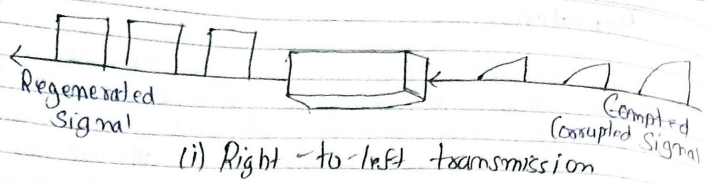
As signals travel along a network cable (or any other medium of transmission) they degrade and become distored in a process that is long enough, the attenuation will finally made a signal unrecognizable by the receiver. A repeater enable signals to travels longer distances over a network.

Repeaters work at the OSI's physical layer. A repeater regenerate the received signals and the retransmits the regenerated (or conditional) signals on other segments.

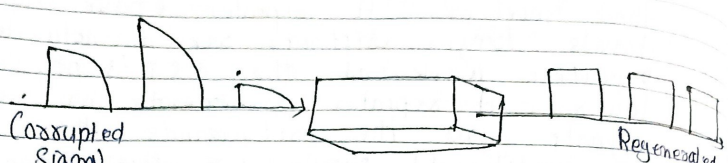
Amplifies cannot discriminate between the intended signal and noise; It amplifies equally everything feed into it. A repeater does not amplify the signal, it regenerates the signal. When repeater receives a weakend or corrupted signal, it creates a copy, bit for bit, at the original strength. Hub is basically a multiport repeater.



Regenerated signal using the Repeater



(i) Right - to - left transmission



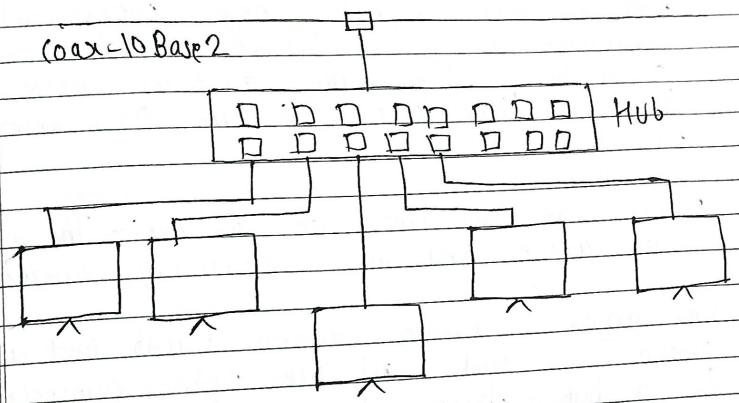
(ii) Left - to - right transmission

Function of a Repeater

Hubs :-

Hubs are used in Ethernet (IEEE 802.3) network in a similar way to that in which are used in Token Ring network. The electronics in hubs need to be more sophisticated however because a signal received at any port must be "instantly" retransmitted on all other port for the CSMA/CD access method to work. Network segments that employee hubs are often described as having a star-bus network topology in which the hub forms the wiring center of the "star".

In early computer networks, needs were connected together in daisy-chain fashion once, all the nodes were connected, each end of the cable could be closed with a terminate. The main problem with this design was that a break anywhere in the cable meant that the network would not function, and one of the major overheads was the time spent in locating the each node has its own connection to the hub, and if the connection fails only that node is affected.



Typical hub is used to connect the Different Nodes

Switches:

The switch is a relatively new network device which is beginning to be used in local Area Network either in place of in combination with hubs unlike hubs, which broadcast message to all ports regardless of the destination address, switches use internal address tables to route frames to only the port associate with the recipient node.

Switches can be used to connect single network needs or entire network segments and in this respect they superficially resemble a cross between a hub and a Bridge. Technically, switches work at the Data link layer of the OSI Reference model.

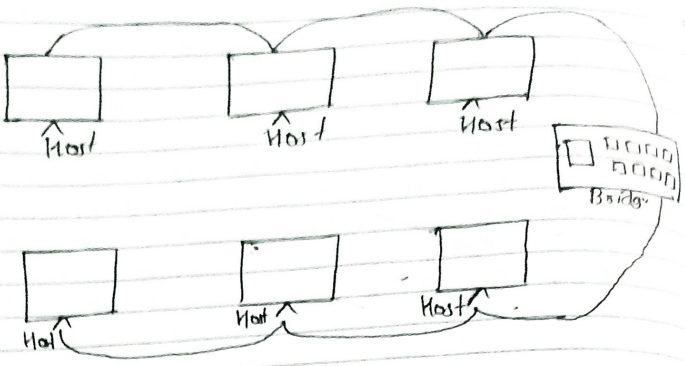
There are two kinds of switches:- The work group switch and the enterprise switch.

One major difference between a hub and a switch is that all the nodes connected to a hub share the available bandwidth, whereas port has the full bandwidth to itself.

Bridger :-

Like a repeater, a bridge can join segments or workgroup LANs. However a bridge can also divide a network to isolate or problems.

Network bridges can be used to connect LAN segments or to isolate heavily trafficed segments from the reset of the network. Bridges operate at the data link layer of the OSI reference model. A bridge both filters and passes packets between network segments.



* Types of bridges :-

Three types of bridges are used in networks:

1) Transparent bridges :- Derives its name from the fact that the device on the network are unaware of its existance. A transparent bridge does nothing except block or forward data based on the MAC address.

2) Source route bridge :- Used in token ring network. The source route bridge from devices its name from the fact that the entire path that the packet is to take through the network is embedded within the packet.

3) Translational bridge :- Used to convert one networking data formal to another for eg. from Token Ring to Ethernet and vice versa.

Routers :- In an environments that consists of several network segments with differing protocols and architectures a bridge might be inadequate for ensuring fast communication among all segments. A network this complex needs a device that not only knows the address of each segment, but for sending data and filtering broadcast traffic to the local segment. Such a device is called a "routers".

- Data is sent to the router.
- The router determine destination address and it to the next step in the Journey.
- The data reaches its destination.

Gateways :- A gateway is a network node used in telecommunication that connects two networks with different transmission protocols together. gateways server as an entry and exit point for a network as all data must pass through or communicate with the gateway prior to being routed. In most IP-based networks, the only traffic that does not go through at least one

gateway is traffic flowing among nodes on the same local network. default gateway or network gateway may also be used to describe the same concept.

The primary advantage of using a gateway in personal or enterprise is it simplifies internet connectivity into one device. In the enterprise, a gateway node can also act as a proxy server and a firewall. Gateways can be purchased technology retailers, such as best buy or rented through an internet service provider.

- Data is sent the router.
- The router determined the destination address and forward it to the next step in the journey.
- The data reaches its destination.