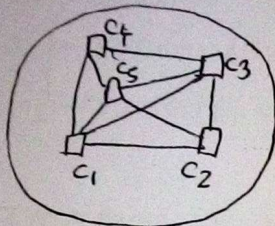


9/1 (1)

COMPUTER NETWORK

→ Data Communication & networking by Fraumen.



Network is an interconnection b/w autonomous machines (independent)

- Fully independent means no master-slave relationship or client-server one.
- All machines are sharing information only thus forming a network & they do not share peripheral devices or OS or memory or software or hardware whereas client-server relationship shares all.

COMMUNICATION

→ Sharing of information.

- TELE COMMUNICATION :- telephonic exchange of data (only voice info is shared)
- DATA " :- exchange of data (info of all types - file, text, audio, video & other special files) info
- LOCAL SHARING → face to face comm.
- REMOTE " → over the distance.

EFFECTIVENESS OF DATA COMMUNICATION :-

It is measured by following components :-

- 1) ACCURACY :- Accurate data should be delivered
- 2) CORRECT DELIVERY :- Delivery to correct destination
- 3) PROPER TIMING :- Delay should be minimum
- 4) JITTER :- No filtering of packets (the sequence in which data is sent should be same when delivered).

A packet has a header & a trailer. The header contains the destination address & trailer contains the data about next packet id to be allocated attached.

COMPONENTS OF DATA COMMUNICATION

- 1) Sender
- 2) Receiver
- 3) Message
- 4) Channel/Medium

Sender $\xrightarrow{\text{Message}}$ Receiver

Channel/Medium

- Wired (Visible) :- Using hardware components
- Wireless (Invisible) :- satellites, radio waves

AMP

PROTOCOLS :- Are the set of rules that govern the communication. They are the agreement made b/w sender & receiver.

PROTOCOL $\rightarrow$ what (sender receives message)
 $\rightarrow$ when (timing)
 $\rightarrow$ how (channel)

KEY ELEMENTS

- SYNTAX :- defines the format of data
- SEMANTICS :- Defines the method of decoding the pattern
- TIMING :- Defines when data should be sent & how fast.

H E Z Z O
1 2 3 4 5

Head $\rightarrow$ [H] $\rightarrow$ Tail

SYNTAX OF
DATA

[O X]

Receiver
should know when
to terminate with
semantics.

$\rightarrow$ Rec Decoding required at receiver end (semantics)

when protocols
Standard
- DEFA

When protocols are documented, they become a standard.

Standards

- DEFACTO (By fact) :- They are not governed by any gov. Locally formed & used.
- DEJURE (By law) :- Defined by governing body & everybody is obliged to follow the rules.

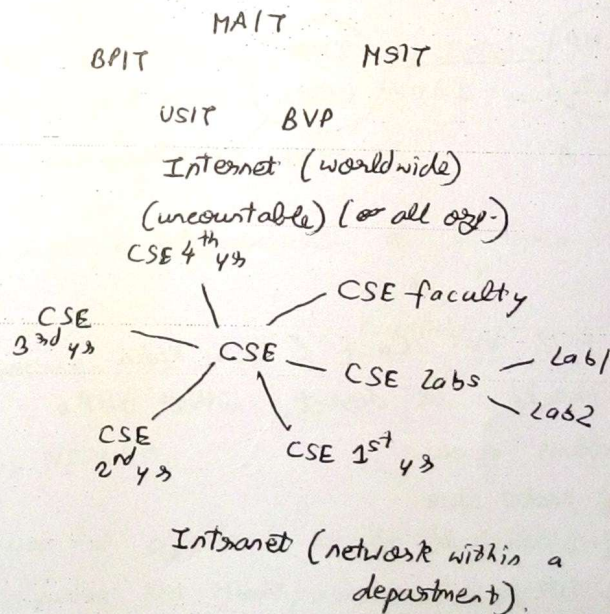
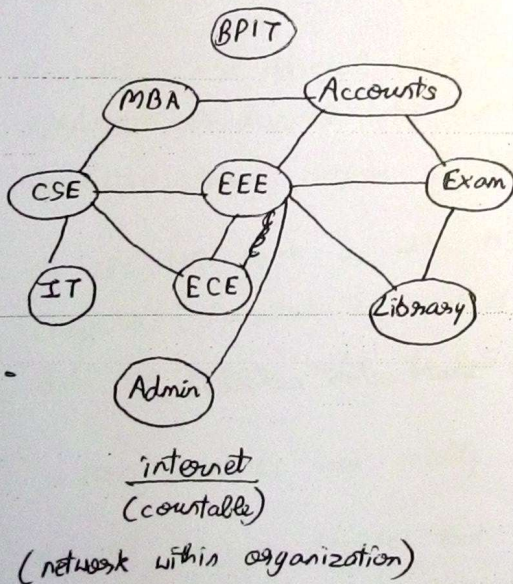
DATA FLOW B/W SENDER AND RECEIVER :-

3 methods :-

- 1) SIMPLEX COMMUNICATION :- $A \rightarrow B$ A to B or B to A (single flow)
- 2) HALF DUPLEX " :- $A \rightleftharpoons B$ A to B or B to A (one at a time)
- 3) FULL " :- $A \leftrightarrow B$ (simultaneously)

INTERNET :- It is a type of network which interconnects many computer networks, where only information is shared. The computers are autonomous in nature.
Interconnection of uncountable no. of autonomous machines.

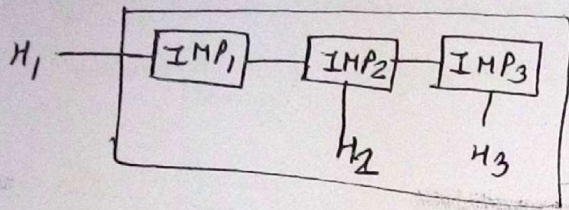
internet :- Interconnection of countable no. of autonomous machines.



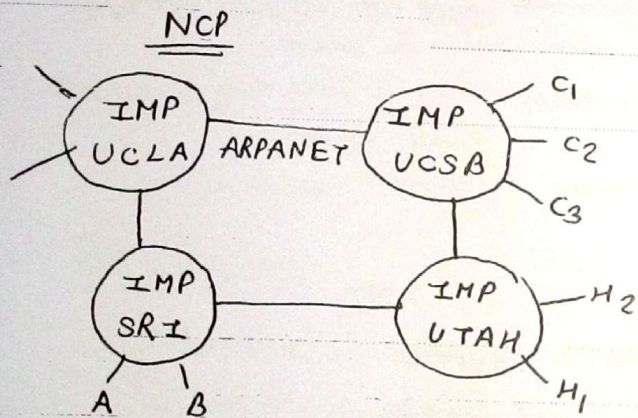
HISTORY OF INTERNET :-

- In mid 1960's, there were standalone labs. There were no sharing of information or no network.
- ARPA → Advanced research project Agency
- Department of Defence of ARPA → in 1967 organised a meeting of ACM presented an idea of small network called ARPANET. Idea was

"each host computer will be connected with special computers, — IMP (Interface Message processor, serves for searching message) & all the IMPs should be interconnected. The interconnection of small IMPs will form ARPANET."



In 1969, ARPANET became a reality in which 4 universities (University of California & Los Angeles, University of California at Santa Barbara, University of Utah & Stanford research institute.) The 4 universities were connected to each other forming ARPANET & the protocol followed was NCP (Network Control Protocol).



12/1

In 1972, Vint Cerf & Bob Kahn presented idea that inter connection b/w host should be direct without IMPs.

Some problems occurs :-

- 1) Diff. packet size
- 2) Diff. transmission rate
- 3) Diff. interface
- 4) Diff. reliability requirements

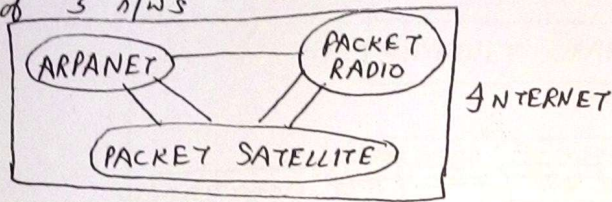
So to overcome these problems, GATEWAY was designed & its purpose was synchronization.

gateway is
and main p

gateway is a device that is used in and main purpose is synchronization.

In 1973, NCP was replaced by TCP (Transmission Control Protocol) where it is responsible for error handling & correction. ARPANET was handed over to DCA (Defense communication agency).

In 1977, TCP was replaced by TCP/IP. TCP can't handle packets. IP handles datagrams (packets). So first internet was formed that consists of 3 n/w's



In 1980, a new OS UNIX came in the market.

In 1981, OS was changed to UNIX for networking coz UNIX was open source OS. CCNET sponsored by National Science Foundation was created less expensive & the transmission rate is low.

In 1983, a new official name was assigned to ARPANET, that was Internet. ARPANET was divided into 2 groups: MILNET & ARPANET where MILNET was used for military purpose & ARPANET for non-military users.

In 1986, NSF came up with NSFNET, was a interconnection of 5 super computers located in centres of US. Data transmission rate of 1.544 mbps.
 thinking capability.

In 1990, ARPANET was totally replaced by NSFNET.

In 1991, US govt. decided that NSFNET was not capable to handle the increasing traffic so came up with ANSNET. 3 companies IBM, Merit, MSI created a new high speed Internet using advanced network service known as ANSNET.

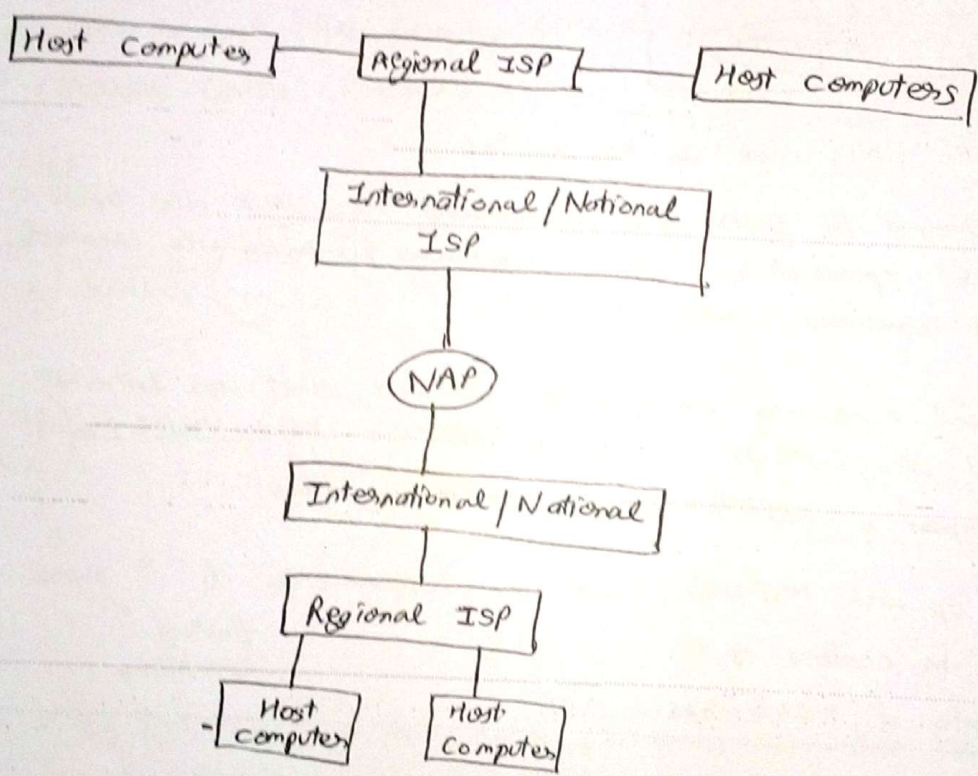
Internet used today is enhanced version of ANSNET.

In 1995, NSFNET was converted to research projects.

- 1967 - Idea of Arpanet
- 1969 - Ap. Market
- 1972 - Gateway
- 1973 - NCP → TCP
- 1977 - TCP → TCP/IP
- 1980 → UNIX
- 1981 → UNIX with TCP/IP, CSNET
- 1983 → ~~Ar~~ ARPANET → INTERNET.

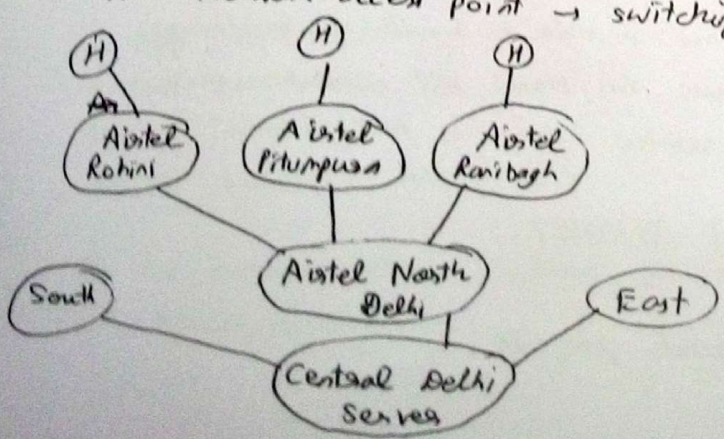
7/2

STRUCTURE OF INTERNET :-



ISP - Internet Service Provider

NAP - Network access point → switching stations (similar to gateway)



18/1

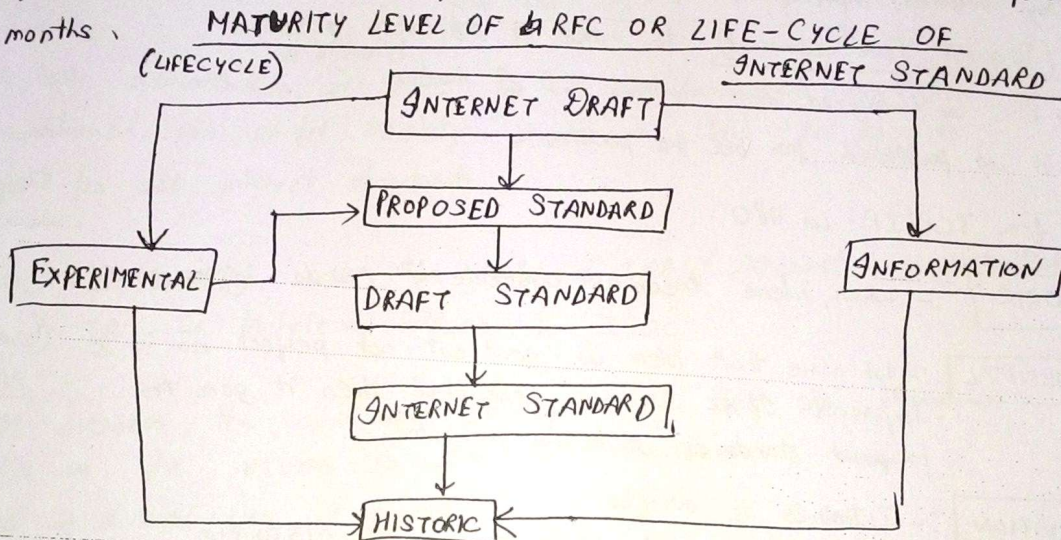
COMPUTER NETWORKS

INTERNET STANDARD

→ Thoroughly tested specifications which everyone who uses internet has to follow them strictly.

→ FIRST we propose a problem statement by ^{draft} group for 6 months (MINIMUM PERIOD).

→ Draft is a document that defines the rules which is studied for 6 months.



→ Idea to change existing methodology & tells diff ways to do it.

INTERNET DRAFT :- Problems fetched in currently executing rules & regulations & the idea that comes that it can be better one. When such ideas are noted on a paper is called INTERNET DRAFT.

→ (THIS CAN BE A BETTER WAY).

PROPOSED STANDARD :- When we try to calculate solution of the ideas in draft & we start working for the solutions.

→ It is stable specification on which the research has started from draft & it is of interest on internet society.

→ It gives solution of the problem.

→ It is worked on for minimum 6 MONTHS & is to be implemented by several groups.

→ If at least 2 groups says that it is successful then we go to next stage i.e. draft standard otherwise it goes to HISTORIC ~~For also it didn't work~~

DRAFT STANDARD :- More refined ~~specification~~ solution to the problem.

- Period of 4 months with stress testing (to test the specifications beyond limits).

- If 2 group gives positive feedback then it gets official name & it becomes INTERNET STANDARD. It means that it had become thoroughly tested specification of ~~now every~~

INTERNET STANDARD

- stable, thoroughly tested specification.
- Now it has to be published.
- Every internet standard is published then & known as RFC (Request For comment). to make it available globally.
- Every RFC is assigned a unique ID & number.
- Now it is published for all the parties.

RFC for TCP/IP is 1180.

HISTORIC :- When ideas becomes obsolete & needs improvement.

EXPERIMENTAL :- When we think idea is good but not perfect so it is improved. If it becomes beneficial then it goes to proposed standards otherwise rejected.

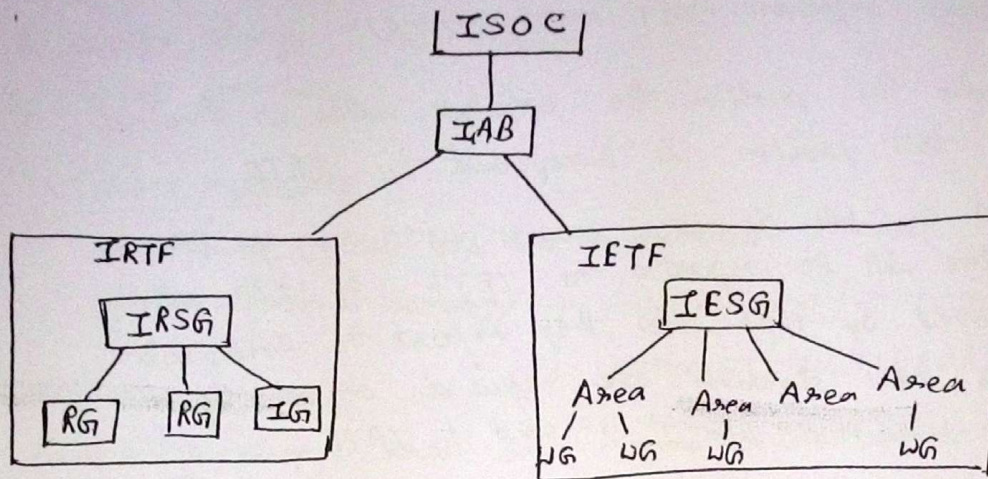
INFORMATION :- Tutorials of drafts.
- When information gets old it is send to HISTORIC.

REQUIREMENT LEVEL OF RFC

5 requirement level :-

- 1) REQUIRED (Mandatory) :- Must for internet communication. Ex:- TCP/IP.
- 2) RECOMMENDED :- Not mandatory but useful. Ex- FTP
- 3) ELECTIVE :- Depended on user's use. Ex:- Encryption.
- 4) LIMITED USE :- RFC that are used in limited situations - Ex. Research
- 5) NOT REQUIRED :- Ex:- Historic

INTERNET ADMINISTRATION :-



- The basic administration of internet is done by ISOC (Internet Society). It is international non-profit society found in 1992 to provide support for all internet standards.

- ISOC is working with the help of IAB (Internet Administrative Board). IAB is technical advisor to ISOC.

IAB :-

- It oversees the continuous development of all the standards & acts as the advisor to all the committees.

IAB is divided into 2 groups :-

- Internet Research task force (IRTF)
- Internet Engineering task force (IETF).

IESG

IESG → Internet Engineering Steering group.

It deals with all the operational problem of internet & proposes solution to the problem.

- They are further divided in working groups known as AREAS.
- Each area concentrate on a specific topic. Currently there are

9 areas-

- Applications
- 2) Internet Protocols
- 3) Routing
- 4) Operations
- 5) User services
- 6) Network Management
- 7) Transport
- 8) Internet Protocol next generation
- 9) Security.

Area further contains appointed WG (Working group).

If the problem to solve the problem the existing rules or standards are not good then that problem is transferred to IRTF.

Users are present in WG. If WG arrives with any problem then first that problem will be reported to IETF. If that problem is not being diagnosed by them then they report to IAB.

IAB checks whether new standards are required or not. If new standards are required then it is sent to IRTF.

After problem is solved.

1912 IRTF → IAB → IETF → IESG → Area → WG.

USES OF COMPUTER NETWORK

used to establish computer network:-

- 1) Resource Sharing : Sharing of device.
- 2) Database Sharing
- 3) Communication among computer/systems :- Chatting
- 4) Sharing of information : File transfer.
- 5) To connect systems/computer in a building
- 6) For education purpose.

Use

- 1) In Business application
 - Sharing of data, database, information, resources
 - Communicating with clients.
- 2) Desktop sharing
 - Telnet - Remote sharing.
- 3) E-commerce.
- 4) Virtual Private Network :- It helps to perform WORK FROM HOME in MNCs.
 - They are connected only to a small group.

- 5) Social Media
- 6) Smart home :- When using all appliances using a remote.
- 7) Globally connecting everyone :- Aadhar Card.

DISADVANTAGE :-

- 1) Personal information is easily available.

↓
Security concern.

- 2) Leading to lot of distraction
- 3) Malware

4) Unwanted
5) Illegal
NETWORK HA
- Transm
- Scale

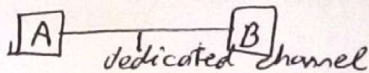
- 4) Unwanted sharing :- Virus, cookies.
- 5) Illegal behaviour

NETWORK HARDWARE

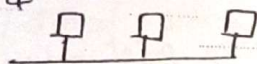
- It deals with how to establish network.
- Transmission Technology
 - Point to point / UNICAST
 - Multipoint / MULTIDROP / BROADCAST
 - Scale.

POINT-TO-POINT :- When some communication channel is shared b/w sender & receiver & this channel is dedicated channel.

[i.e. only sender & receiver can use it no one else can interfere with that link].



MULTI-POINT :- A channel is shared by 1 sender & many receivers & vice-versa.



SCALE :-

On the basis of scale, network can be of 4 types :-

- PAN
- LAN
- MAN
- WAN

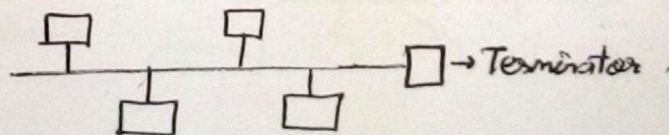
NETWORK TOPOLOGIES :-

It is a geometric representation of the relationship of all the links in the network. Network Topology describes the layout or the appearance of network i.e. how computers, cables & other components are interconnected both physically & logically.

(how systems are kept?) (how data will flow).

TYPES :-

1) BUS TOPOLOGY :-



- Multidrop connection but communication is point to point (channel capacity is shared b/w multiple users).

- Scenario :- PUSH & PULL to send & receive message. Source will push the message to channel capacity, then all b/w systems will check pull it, if its not of itself then it will push it otherwise will pull it.

terminator will tell that bus topology is completed.

Messages are always transmitted in forward direction.

If message reaches to terminator, it means that is not of any previous systems. Now terminator will send the information to the starting system in bus topology.

If any information is not pull by any system & then that message reaches to sender. At that time, sender will only pull the message & will discard it.

→ It is applied in single room.

It is of 2 TYPES :-

- REGULAR BUS :- All machines are fixed at starting point only. So no new machines can be arranged without re-installing it. FIXED NUMBER OF CONNECTION.
- LOCAL BUS

↓
ADHOC TECHNOLOGY :- Here temporary topology is arranged b/w machines. Now when desired information is transferred that topology is discarded.

→ CONNECTIONS CAN VARY

FEATURES OF BUS TOPOLOGY :-

- ∴ Signal circuit to which all the devices are connected.
- ∴ Multi-drop connection.

ADVANTAGES :-

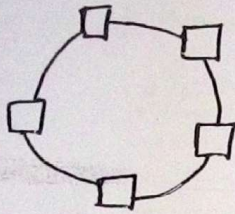
- ∴ Easy to understand & easy to install.
- ∴ It requires less wire for connection.
- ∴ No central point.
- ∴ Easy to expand.
- ∴ Signal strength is maintained.
- ∴ Fault isolation is easy.

DISADVANTAGES :-

- ∴ If any problem in main wire, complete system will shut down.
- ∴ Speed is very slow.

∴ Maintenance cost is high. [It is difficult to diagnose fault].

RING TOPOLOGY :-



- Multi-drop connection in which ^{message} communication is broadcasted.
- Pull & ignore.
- Used where high performance is required.
- Here whenever an information is sent it is sent with a time interval, if it is fetched in that particular time interval then info is fetched otherwise it is discarded.

FEATURES :-

- * Direct transmission of message
- * Only the receiver receives rest ignores message.

ADVANTAGES :-

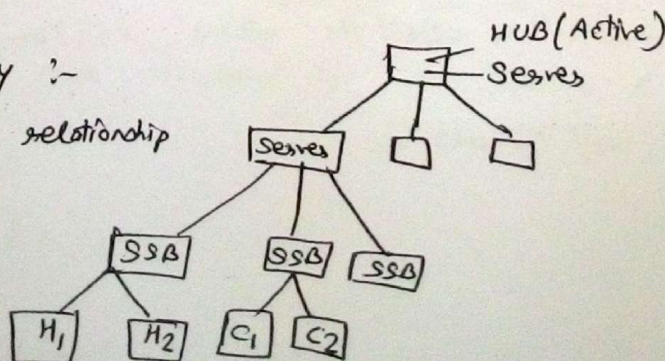
- * System growth is easy
- * All system have equal access.
- * Data packet travel at greater speed.
- * Congestion

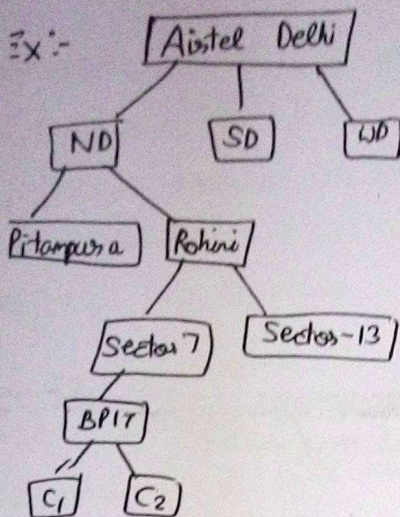
DISADVANTAGES

- * Congestion is high.
- * If 2 machines want to traffic at same time, it will cause congestion.

TREE TOPOLOGY :-

→ parent-child relationship

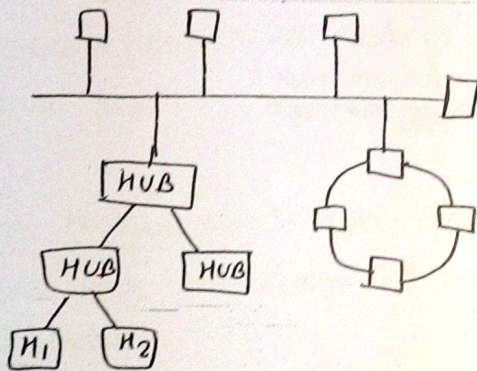




DISADVANTAGE
→ System

HYBRID TOPOLOGY

- used for establishing the internet.



ADVANTAGES :-

- Expansion is very easy
- failure at 1 node doesn't affect the entire system
- easy to install & easy to use.

DISADVANTAGES :-

- System is very complex.
- Large no. of wires are required.

$$\frac{n(n-1)}{2} \quad n \rightarrow \text{devices}$$

- each link has a dedicated bandwidth. So huge bandwidth wastage is there.
- Scalability is difficult.

Q.7 An education lab has fully connected mesh topology consisting of 10 devices. Calculate the no. of cables to establish mesh topology & calculate the no. of ports required by each computer.

$$n = 10$$

$$\frac{n(n-1)}{2}$$

$$= \frac{10 \times 9}{2}$$

$$= 45$$

$$\begin{aligned} \text{No. of ports by each device} &= \frac{n-1}{1} \\ &= 9 \end{aligned}$$

Q.7 Assume 7 devices are to be arranged in a room. Calculate the no. of links & ports required by Mesh Topology & compare it with ring topology.

$$\text{links} = \frac{7 \times 6}{2} = 21$$

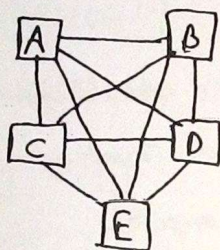
$$\text{Ports by each device} = 6$$

DISADVANTAGES :-

- Totally dependent on hub
- Cost of hub is very high

MESH TOPOLOGY

Each device has a dedicated point-to-point link to every other device on the network.



No. of wires required to establish the mesh topology are

$$= \frac{n(n-1)}{2}$$

ADVANTAGES :-

- loss of information is minimum
- reliable system as every system has dedicated link.
- fault identification is easy.
- fault isolation is also easy.
- ~~is~~ ideally used in real time scenario
(alternate path are also available).

NETWORK RANGE :-

Range is a physical size of the network - Acc. to size of network the network is classified in 4 categories :-

- | | <u>Range</u> |
|-------|--------------|
| - PAN | 1m |
| - LAN | 10m - 1km |
| - MAN | 10km - 180km |
| - WAN | over 180km |

→ 10,000km over → known as internet.

PAN → Personal area network

- personal use
- ~~Ex~~ One to one connection
- Ex:- using printer, ~~to~~ bluetooth connection

LAN

- Local area network
- When network is established within a room/lab.

→ now

- For establishing LAN :-
 - routers
 - repeaters
 - computers
 - wires

- network interface card
- other peripheral devices.

FEATURES :-

- max. transmission speed (as distance is less)
- less complexity
- cheap (configuration is easy to install)
- fault detection & isolation is easy.
- delay is minimum.
- uses broadcast technology.

- reliability in LAN is high (following direct path)
- Peripheral devices can only be used through LAN

MAN

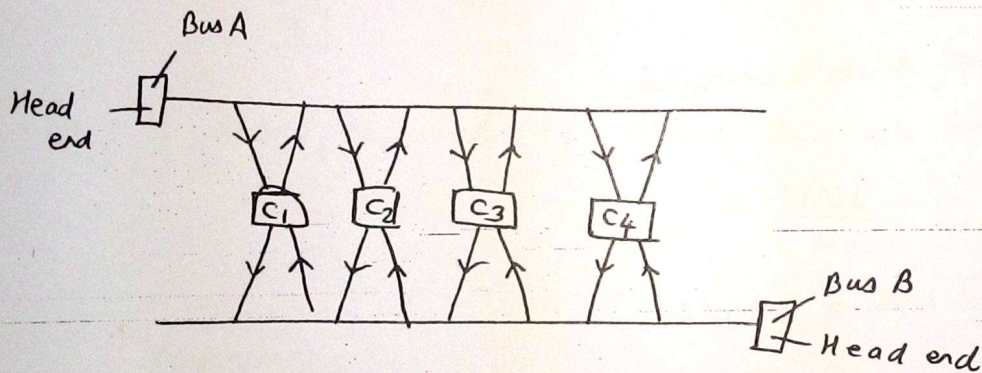
- Metropolitan area network

Ex:- Cable network

- To increase the transmission speed of MAN, a new standard was developed.

IEEE 802-6

DQDB → Distributed Queue Dual Bus

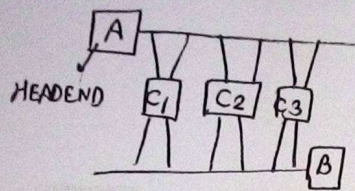


WAN

- wide area network

P.T.O.

At the time of configuration, it is decided whether connection is upstream (connected with upper bus) or downstream.



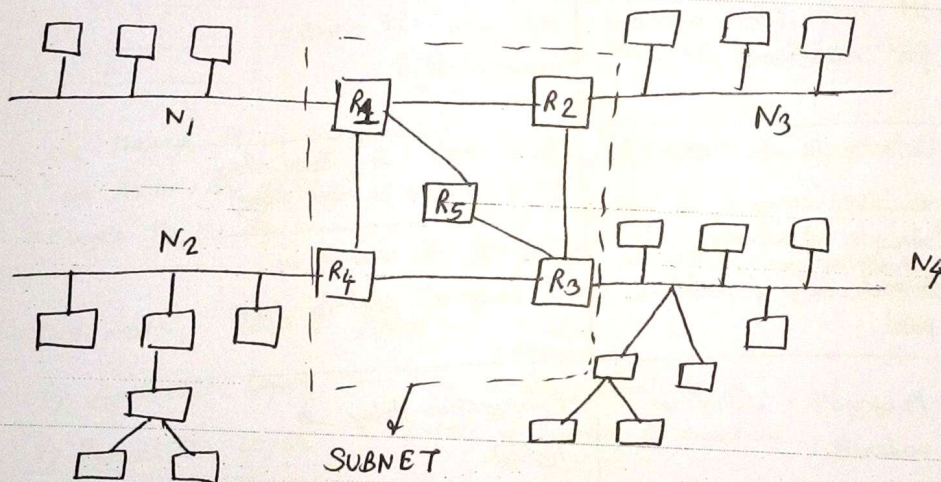
→ If C_1 is connected upstream then bus A (upper bus) is primary bus & lower bus is secondary bus.

→ System is right of C_1 to transfer data to the system right of C_1 , upstream is used & for left of C_1 downstream is used.

→ Whenever we want to transfer data through bus, headend will decide whether data is to be transferred from bus or not.

WAN (WIDE AREA NETWORKS).

→ Connecting multiple MANs.



→ ROUTERS are used that ~~from~~ decides the path for the information so that it reaches destination.

→ In WAN, connection is established between routers.

→ Now routers are responsible to transfer data among their network.

→ As distance is very large so it is not possible to connect all systems hence routers are used.

→ SUBNET has 2 basic components :-

1) TRANSMISSION LINES are responsible for transferring message to respected routers.

2) SWITCHING ELEMENTS are specialized computers used to connect 2 or more transmission lines.

not path & no one else can use it. Also if a router is performing some other work prior to this one then first router will complete that work & then will transmit this one.

MECHANISM :- Store & forward point to point.

SUBNET MASK :- Address of subnet.

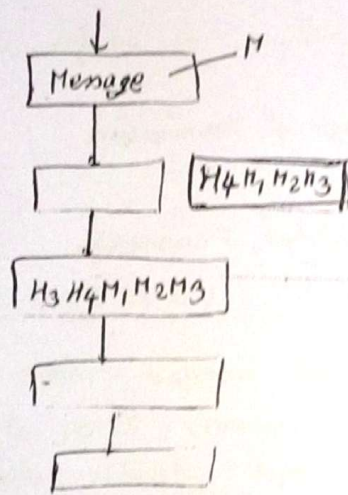
Default subnet mask is 255-255-255-0.

<u>LAN</u>	<u>MAN</u>	<u>WAN</u>
Used for private networks.	Used for private & public networks.	Used for private and public networks.
LAN is established in smaller area.	MAN is established in moderate area.	WAN is established in wider area.
Design is very easy.	Design is bit tricky.	Design is highly complicated.
It uses coaxial & twisted pair cables connections.	It uses fibre optic for connections.	It uses satellite communication.
Data rate is high.	Data rate is moderate.	Data rate is slow slow (As distance is very large).
Principle of working is broadcasting ^{multitasking} & point to point.	Principle of working is broadcasting ^{multitasking} & point-to-point.	Principle of working is switching & point-to-point.
Propagation delay is negligible.	Propagation delay is moderate.	Propagation delay is highest.
Error rate is lowest.	Error rate is moderate.	Error rate is highest.
Equipment for LAN is less expensive.	Equipments are more expensive.	Equipments are most expensive.
Most suitable for critical applications.	Less suitable for time critical applications.	Least suitable for time critical applications.

Layered Approach:-

- Staircase approach
- Output of first layer is input of next layer.
- First message goes to topmost layer.

→ Whenever a layer processes the message that is taken from another layer, it adds a signature (header) to the message.



As Message M is bigger, it is broken into different messages M_1, M_2, M_3 .

In network architecture, we will study 2 model models:-

- OSI Model
- TCP/IP Model.

OSI (OPEN SYSTEM INTERCONNECTION/INTERFACE MODELS)

- It was introduced in late 1970.
- It was designed by international organizations standard.
- It is a set of protocols that allows any 2 system to communicate + regardless of their architecture.

→ OSI models has 7 layers. ^{sender} _{receives}

- 1) Application Layer → For sender, first layer
- 2) Presentation Layer → interface of human & machine.
- 3) Session Layer
- 4) Transport Layer
- 5) Network Layer
- 6) Data Link Layer
- 7) Physical Layer → For ^{receiver} _{sender}, first layer.

• APPLICATION LAYER

- also known as HUMAN LAYER.

- It takes message from the sender, thus human interacts in this layer.

• PRESENTATION LAYER

- presents the layer for communication.

- It finalizes the syntax as well as data compression.

PHYSICAL
- It converts
- After c
- It activates

- Data Presentation :- Conversion from native form to common form.
- Data compression :- Layer is responsible to reduce volume of data.
- Encryption :- Layer is responsible to hide the details of message.

- It only sends text to ^{next} ~~further~~ ~~layers~~ layer.

INTERFACING BETWEEN 2 LAYERS means when message is transferred from 1 layer to next one.

SESSION LAYER

is responsible for establishing, maintaining & termination of session.

- Now to provide collision whenever a machine establishes a connection with session, no other machine will interface with it.

~~It is~~

It is responsible to maintain the exchange of informal message b/w computers.

It is also responsible for synchronization.

It is function of this layer to insert checkpoints.

Checkpoints ^{acknowledges} ~~tells us~~ that at this position data or message is ~~receive~~ received.

• TRANSPORT LAYER

~~It decides whether transportation will take place on a sin~~

It decides whether complete transmission of message will take place on a single path or on multiple paths.

It allows multiple paths. (MULTIPLEXING)

It divides the data into small groups.

NETWORK LAYER

It is responsible for proper networking routing b/w source to destination.

It acts as a network controller.

DATA LINK LAYER

- It deals with error detection & error correction

- It divides packets into frames.

(As in networking, frames of message are transmitted, not the packets).

PHYSICAL LAYER :-

- It converts ^{frame} message to machine language.
- After converting into bits, it converts message to electrical signals.
- It activates, maintains & deactivates ~~mess~~ physical connection.
- It decides whether communication is simplex, half-duplex or full duplex.

TRANSMISSION MEDIA :-

It can be defined as anything that carry information from source to destination.

2 types :-

1) GUIDED TRANSMISSION MEDIA :- Contains signal energy & guided within a solid media.

- point to point communication
- Discrete network topology

- additional transmission ^{capacity} can be added by using more wires.

2) UNGUIDED TRANSMISSION MEDIA :- Signal energy propagates through electromagnetic waves.

- for broadcasting.
- continuous network topology
- It is not possible to procure additional capacity.

GUIDED MEDIA TYPES

1) TWISTED PAIR :-

orange - white of orange (O-o)

blue - (Bb)

green - (Gg)

brown - (B₂ b₂)

SWITCHING :-

- It helps to connect devices via switches.
- SWITCHED NETWORK :- Workstation, servers are connected via switches.
- They are not bothered by of data.
- HUB are active component whereas switches only transfer data.
- The fundamental of working of switches is STORE & FORWARD.
- Here only receiver will get the data by the help of tokens.
- SWITCHING :- Concept how switches work in switched network.

SWITCHING are of 3 types :-

- CIRCUIT SWITCHING :- Before transmission of message, connection is established
- MESSAGE SWITCHING :- No path establishment, a message is send directly from sender to receiver.
- PACKET SWITCHING :-

I/ CIRCUIT SWITCHING :-

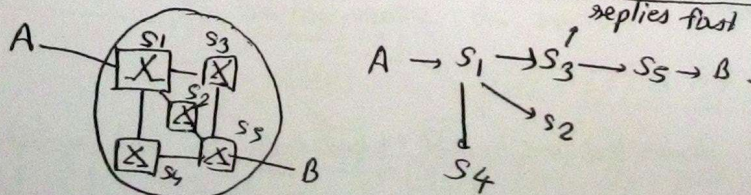
Types :- Different phases are :-

1. Connection established :- Here first switch will send the ~~same~~ a message to all its connection if it is not directly connected with destination.

Now the switch (S_2) that will send the reply first to with the first switch is included. So, S_2 will check whether it has a path connected to destination.

As so, path that gives reply first ~~is~~ given higher priority

→ Here, simply path is as connection is fixed. # Data is not transferred. This is known as PATH ADVERTISING.



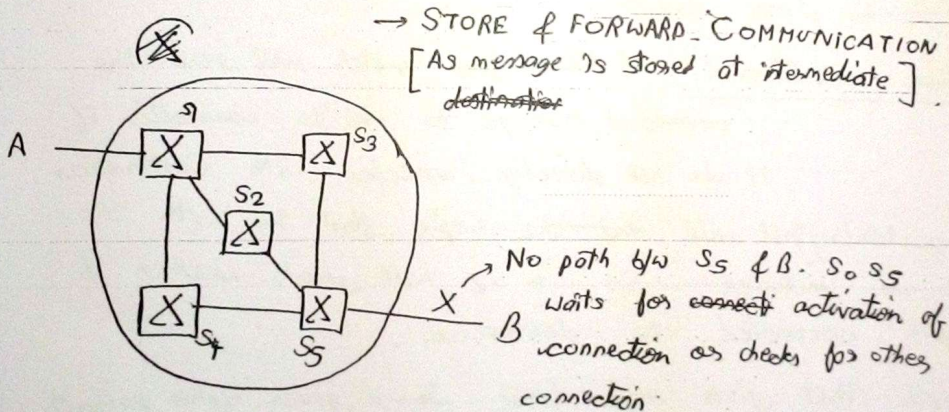
2. DATA TRANSFER :-

- Since in previous steps, all switches are fixed so they cannot be used to transfer other data.
 - Hence it is time consuming as first connection is fixed, then data is transferred.
- DISADVANTAGE
- It also takes large can also take large bandwidth for smaller message even. As whole message is transferred at a time (not divided into diff. packets) so memory is wasted as it is fixed. Channel bandwidth is wasted.

3. TERMINATION

ADVANTAGE :- data is not stored.

I MESSAGE SWITCHING :-



→ Not reliable way of switching as here no acknowledgement is sent to sender whether message is received or not.

ADVANTAGE :-

- Path is not dedicated. Channel bandwidth is not wasted. It is properly used.
- Proper traffic management.
- Congestion minimized.

CONGESTION
- No limit
space the
a waste

CONGESTION :- Path is not available or congested.

- No limit on block size. So if switch does not have that much space then that message gets truncated. Hence message becomes a waste.

III. > PACKET SWITCHING :-

The message is divided into different packets & each packet can follow different path.

ADVANTAGE :-

- delay is minimized
- bandwidth is properly optimized.
- ~~Not~~ Not time consuming.

- Each packet will have a header which will contain details of receiver.

1. > DATAGRAM PACKET SWITCHING :-

Message is divided into different datagram & each datagram is sent through different routes.
[Packets are known as DATAGRAM].

2. > VIRTUAL CIRCUIT SWITCHING :-

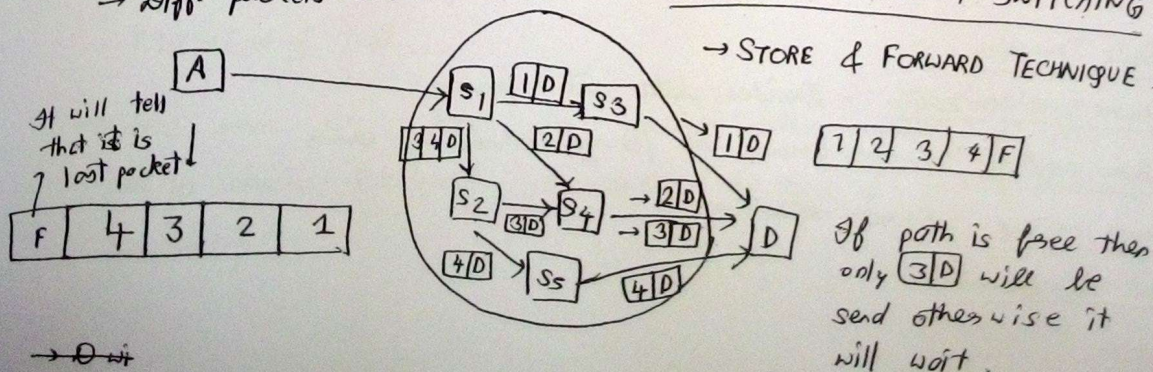
A virtual circuit is created before the actual data is sent.

→ No. of packets are divide numb

→ Diff. packets are numbered.

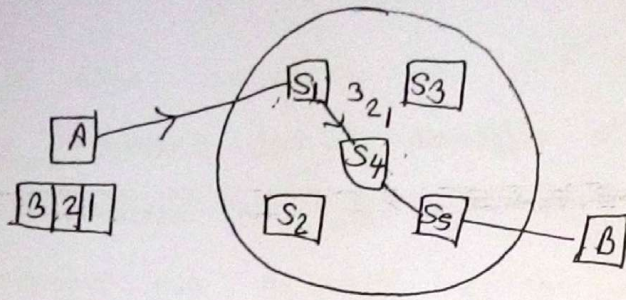
DATAGRAM CIRCUIT SWITCHING

→ STORE & FORWARD TECHNIQUE.



2) VIRTUAL CIRCUIT SWITCHING:-

It is a combination of circuit switching & datagram switching.



Here first each switch will check & establish the connection. Then that connection will get freeze. Now after connection is fixed, message is divided into different packets known as datagram. These message switch S_1 will transfer all the packets after some duration to the next switch. Now here next intermediate switch S_4 will send the packets to next one.

✓ Acknowledgement of single packet is taken

② UNIT 2 :-

DATA LINK LAYER:-

- Second last layer of OSI
- last layer of TCP/IP.

Functions are :-

- ↳ Data Transfer
- ↳ Frame synchronization :- Divides data into frames
- ↳ Flow control :- Proper frames are flowing without any errors.
- ↳ Error control :- Error detection
- ↳ Link Management.